КИТ МАРТИН

КРИПТОГРАФИЯ

КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ

АЛГОРИТМЫ ШИФРОВАНИЯ | МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ | ПРОТОКОЛЫ БЕЗОПАСНОСТИ

БОМБОРА
ИЗДАТЕЛЬСТВО

Введение

Ею пользовался Юлий Цезарь. Ее пыталась применять Мария Стюарт, но не справилась и лишилась головы. Наполеон ею злоупотреблял, и это стоило ему империи. На нее полагались все стороны Второй мировой, и многие считают, что именно превосходство союзников в ее применении позволило войну наконец закончить. На протяжении всей холодной войны без нее не могли обойтись шпионы и разведчики, более того, и сейчас не могут. Но кое-кто использует ее намного чаще и для неизмеримо более широкого круга задач. Кое-кто полагается на нее при решении значительной, если не большей части своих повседневных задач. Этот человек – вы. А этот незаменимый инструмент – криптография.

Именно криптография обеспечивает безопасность множества обычных дел, которые лишь на первый взгляд не нуждаются в защите. Вы обращаетесь к ней, когда звоните по мобильному, снимаете наличные в банкомате, подключаетесь к сети Wi-Fi, входите в систему компьютера, ищете информацию в Google и смотрите фильмы в Netflix. Криптография помогает защитить более миллиарда устройств Apple[1], более 7 миллиардов банковских карт[2] и 55 миллиардов ежедневных сообщений WhatsApp[3]. Цифровая валюта Bitcoin и сопутствующий блокчейн тоже опираются на криптографию.

Собственно говоря, криптография ответственна за защиту более трех четвертей всех глобальных соединений в Интернете[4]. Известно ли вам, что при подключении к безопасному веб-сайту ваш браузер использует криптографические инструменты, без которых не произошла бы компьютерная революция, создавшая Интернет в его нынешнем виде? Знали ли вы, что каждый раз, когда вы открываете дверь автомобиля, ваш ключ делает то, на что не способен ни один злоумышленник с доступом к самому мощному суперкомпьютеру в мире? Можете ли вы представить, что сообщения с вашего телефона зашифрованы так хорошо, что это может всерьез обеспокоить некоторые разведслужбы?

В сущности, криптография – это одно из практических применений математики. Но сложно назвать хотя бы еще одну область, где

математика применялась бы в таких масштабах и была бы настолько важной. Ей редко уделяют внимание в популярных фильмах, но с криптографией все иначе: вспомните *Энигму, 007: Координаты «Скайфолл»* и *Тихушников*[5]; или сериалы *C.S.I.: Киберпространство* и *Призраки*[6]; или такие бестселлеры как *Цифровая крепость* Дэна Брауна[7].

К тому же математика обычно не решает исход войн и не нервирует мировых лидеров.

Криптография предоставляет набор инструментов для защиты информации. Их можно применять к информации, представленной физическим образом, такой как слова, написанные на бумаге, но ее огромная роль в современной жизни объясняется в основном нашей растущей зависимостью от цифровых данных. Криптография позволяет держать конфиденциальную информацию действительно в тайне. С ее помощью можно обнаружить случайное или умышленное изменение информации. Она дает возможность определить, с кем мы общаемся. На самом деле это практически единственное доступное средство для обеспечения цифровой безопасности.

Криптография подобна антибиотикам: их тоже можно принимать всю жизнь, ничего в них не понимая. Однако существуют целых две причины разобраться в том, как они работают. Во-первых, это поможет понять, как устроено человеческое здоровье, и когда антибиотики принимать стоит, а когда нет: такое знание будет полезно как вам самим, так и окружающим. Во-вторых, потребление антибиотиков каждым отдельным индивидом складывается в важные последствия для общества в целом: чрезмерное использование и появление супербактерий.

Точно так же можно всю жизнь применять криптографию, даже не подозревая о ее существовании. Однако я убежден, что даже немного знаний в этой области могут принести огромную пользу. Прежде всего мне хотелось бы открыть вам глаза на ту огромную роль, которую криптография играет в поддержке вашего образа жизни. Мне кажется, что понимание того, зачем нужна криптография и как она работает, позволит вам увереннее ориентироваться в вопросах цифровой безопасности. Кроме того, применение криптографии затрагивает и более широкие социальные вопросы баланса личной свободы и

контроля за информацией, и их я тоже собираюсь исследовать в этой книге.

Киберпространство

Я не стану предпринимать никаких серьезных попыток дать определение *киберпространству*[8]. В контексте нашей книги киберпространство – это все, что вы таковым считаете. Иными словами, все множество «электронных вещей[9]».

Киберпространство состоит из компьютеров, взаимодействующих через сеть, иначе говоря – из устройств, которые можно с уверенностью назвать вычислительными. Это не только стационарные ПК, моноблоки и ноутбуки, но и такие гаджеты, как мобильные телефоны, игровые приставки, и даже голосовые помощники. Эти последние принято считать устройствами с доступом к Интернету, но компьютерами их признают редко. Помимо них киберпространство состоит из миллионов устройств, с которыми мы взаимодействуем напрямую (включая платежные терминалы, банкоматы и системы паспортного контроля), и других, скрытых от нас, например компьютерных систем бизнеса, обороны и промышленного управления.

Наверное, самым важным и до некоторой степени тревожным можно назвать тот факт, что многие устройства, которые даже не принято считать цифровыми, не говоря уже об отнесении их к компьютерам, стремительно расширяют свое присутствие в киберпространстве: автомобили, бытовая техника, «умные дома». Сети, объединяющие их, могут быть проводными и беспроводными, коротковолнового и длинноволнового диапазона, полностью открытыми или выделенными для определенных задач, таких как телекоммуникации. Самой важной из этих сетей, безусловно, является Интернет.

Конечно, между киберпространством и реальным миром нет четкой границы, их элементы взаимодействуют все активнее с каждым днем. Все сложнее найти человека, который не пользуется Интернетом[10], компанию, которая не представлена онлайн, или технологии, никак не

связанные с киберпространством. И при этом большая часть происходящего в киберпространстве – результат нажатия кнопок на физических устройствах, запускающих программы на компьютерах, которые можно пощупать.

Ваша безопасность в киберпространстве

Задумайтесь на секунду, насколько сильно вы зависите от киберпространства. Вспомните, как вы общаетесь с друзьями, где читаете и смотрите новости и как выбираете, где провести следующий отпуск. Как ведете финансы и делаете покупки. Не забывайте о музыке, фильмах, фотоальбомах. Я уже упоминал об автомобиле? Он открывает двери по нажатию кнопки, всегда знает, где находится, отчитывается производителю о неполадках и понемногу учится ездить самостоятельно. И это лишь верхушка айсберга. Каждый день вы полагаетесь на множество незаметных вещей, которые просто работают. Самолеты летают, электричество питает устройства, сигнал светофора меняет цвет. В наши дни киберпространство повсюду.

Вместе с киберпространством в нашу жизнь потихоньку проникают и киберпреступники. Сеть – это чудесное место для совершения преступлений. Не ограниченные расстоянием, злоумышленники в любой точке мира находят возможность совершить налет на ваш дом. Это идеальное место для того, чтобы пускать пыль в глаза: подросток, сидя в своей комнате, может притвориться представителем вашего банка или сымитировать веб-сайт торгового центра. В новостях постоянно мелькает что-то о нарушении безопасности посредством компьютеров – и это лишь то, что на слуху.

Точные цифры установить крайне сложно, но, если верить компании кибербезопасности Norton, в 2017 году в мире было 978 миллионов жертв киберпреступлений (и в общей сложности 172 миллиарда долларов ущерба[11]). Компания профессиональных услуг PwC утверждает, что в 2016 и 2017 годах[12] 31 % случаев корпоративного мошенничества приходился на киберпреступления. А исследования Cybersecurity Ventures говорят о 6 триллионах долларов, в которые киберпреступность обошлась глобальной экономике в 2021 году[13].

Киберпространство по большей части не попадает в наше поле зрения, и мы, как правило, о нем просто не думаем. Это могут подтвердить иранские ученые на заводе по обогащению урана в Нетензе, чьи центрифуги в 2010 году[14] начали загадочным образом ломаться, или руководители Sony Pictures, невольно ставшие в 2014 году звездами собственного фильма ужасов, когда их корпоративная переписка, доходы и еще не вышедшее кино оказались достоянием всей сети[15].

Мы существа из плоти и крови, эволюционировавшие в реальном мире, и мы неплохо ориентируемся в физических средствах безопасности вроде дверей с замками, паспортного контроля, подписанных и заверенных документов и т. п. Но нам с очевидностью не хватает той же степени понимания кибербезопасности. Этому, конечно, способствует виртуальная природа киберпространства, но я подозреваю, что основная причина – отсутствие хотя бы элементарного понимания, что такое эта самая безопасность в киберпространстве. Мы оставляем открытыми настежь парадные двери, передаем незнакомцам реквизиты банковских счетов и высекаем интимные записки на цифровой скрижали, с которой их уже не стереть. Я покажу вам, как криптография пытается решить саму суть этой проблемы и дает возможность принимать взвешенные решения о том, как защитить себя и свои данные.

Понимание основ криптографии поможет вам оценить важность технологий безопасности, которыми вы пользуетесь ежедневно. Пароли применяются повсюду, но и недостатков у них множество. Кстати, знаете ли вы, что ваш онлайн-банкинг, скорее всего, защищен «идеальным» криптографическим паролем? Криптография в конечном счете полагается на секретные элементы, известные как ключи. Я попытаюсь повысить вашу осведомленность о важности этих ключей для вашей цифровой безопасности, и советую вам относиться к ним так же бережно, как и к физическим ключам, а в идеале еще бережней, так как зачастую в киберпространстве ваш ключ – единственное, что отличает вас от остальных 4,5 миллиарда пользователей Интернета. Не правда ли, крайне важно иметь о них какое-то представление и знать, где они хранятся?

Информированность о криптографии также поможет вам адекватно реагировать на проблемы кибербезопасности, с которыми вы сталкиваетесь. Каковы потенциальные последствия подключения к

незащищенной сети Wi-Fi? Так уж ли важны разные пароли для разных учетных записей? Стоит ли продолжать работу с веб-сайтом, у которого нет действительного сертификата? И что насчет всех этих новых историй о кибербезопасности? В 2017 году широко распространилась новость о том, что сети Wi-Fi, использовавшие определенный протокол шифрования, оказались небезопасными[16], и что криптографическое оборудование от Infineon было легко взломать[17]. 2018 год начался с новости о дефектных чипах многих устройств Apple[18]. Пора ли паниковать? Принимать ли меры самостоятельно, или об этом позаботится кто-то другой? Следует ли быть в восторге от блокчейна? Или, может, пора волноваться о квантовых компьютерах?

Элементарные знания по криптографии также помогут вам решить, как обращаться с нынешними и будущими технологиями. Безопасно ли передавать персональную информацию тому или иному приложению? Правда ли вы рискуете потерять все деньги, переводя их в Bitcoin? На что по теме безопасности нужно обращать внимание, выбирая новый телефон?

И это касается не только вас; это общая проблема. Конечно, если вы забудете закрыть дверь и сейф, и вор похитит ваши бриллианты, это будет ваша потеря, а не моя. Но с кибербезопасностью все иначе. Если вы неосторожно щелкнете по подозрительной ссылке на видео с пляшущей овцой, ваш компьютер может легко стать частью глобальной преступной сети и атаковать одно из моих устройств. Так что все мы заинтересованы в том, чтобы вы могли защитить себя в киберпространстве. Если повезет, то каждый читатель, который приобретет немного базовых знаний по криптографии, подарит нам всем капельку безопасности.

Социальная дилемма

Криптография – неотъемлемая часть нашей повседневной жизни, без которой мы уже довольно давно не можем обходиться. Тем не менее в каком-то смысле ее можно назвать хлопотной и даже опасной.

Она работает настолько хорошо, что порождает в обществе социальную дилемму.

В мае 2017 года сетевые администраторы сорока британских больниц оказались в кризисной ситуации. Компьютерные системы, отвечавшие за рутинные операции, вышли из строя, и причиной тому была криптография. Злоумышленники взломали их с помощью криптографических возможностей программы WannaCry и перекрыли доступ ко всем данным. За возвращение систем в нормальное состояние, разумеется, потребовали выкуп. Криптография надежно защищает нас в киберпространстве, но это был один из случаев, когда она, напротив, привела к серьезным проблемам[19].

Как ни досадно, криптография не делает разницы между вашими данными и, к примеру, переговорами преступников, планами террористических группировок и распространением детской порнографии. Неудивительно, что службы безопасности некоторых стран высказывают озабоченность ее повсеместным применением. Особенно этим известен бывший директор ФБР Джеймс Коми, регулярно сетовавший на то, что криптография препятствует сбору разведданных[20]. А в 2013 году бывший контрактник Агентства национальной безопасности США Эдвард Сноуден пожертвовал карьерой и свободой, предав огласке механизмы, с помощью которых АНБ пыталось обойти повседневное использование шифрования[21].

На криптографию порой возлагают и вину за серьезные нарушения безопасности в реальном мире. По крайней мере частично. После теракта в Париже в 2015 году британский премьер-министр Дэвид Кэмерон публично задавался вопросом: «Хотим ли мы позволить в нашей стране средства коммуникации, которые не можем контролировать?»[22]. В июне 2017 года австралийский Генеральный прокурор Джордж Брэндис заявил, что Австралия возглавит международные переговоры о роли промышленности в «борьбе с шифрованным обменом сообщениями между террористами»[23]. Примерно в то же время немецкий министр внутренних дел Томас де Мезьер сообщил о подготовке закона, позволяющего государственным органам читать шифрованные частные сообщения, аргументировав это тем, что государство «не может допустить существование пространства, фактически стоящего вне закона»[24]. А в мае 2018 года Генеральный прокурор США Джефф Сешнс высказался о том, что «с

распространением шифрования и „уходом в тень“ необходимо что-то делать»[25].

Все эти политические высказывания, в сущности, сводятся к требованию снизить эффективность криптографии. Однако верховный комиссар ООН по правам человека, Зейд Раад аль-Хуссейн, неоднократно заявлял о том, что запрет шифрования «может поставить под угрозу человеческие жизни»[26]. Можно ли примирить эти точки зрения?

Сегодняшние споры об использовании криптографии на самом деле продолжают давнюю дискуссию о свободе и контроле за информацией в цивилизованном обществе. Изобретение печатного станка в середине пятнадцатого века породило и борьбу за возможность контролировать книгопечатание. Решая, кто может издавать книги, а кто нет, светские и церковные власти управляли доступом общества к информации[27]. В наши дни криптография защищает потоки цифровых данных так, что это снова вызывает опасения у правительств.

Между свободой и контролем в любом вопросе не бывает простых компромиссов. Многим политикам и журналистам работа над этой темой дается нелегко, так как они, по всей видимости, не понимают, для чего предназначена криптография и как она работает[28]. Я попытаюсь объяснить, какую пользу она приносит и какие трудности создает, чтобы вы могли сформировать обоснованное мнение о ее использовании. Эти знания пригодятся вам не раз, поскольку в будущем наша зависимость от криптографии будет только расти, а социальные трения, которые провоцирует ее применение – обостряться.

Мой подход

Несмотря на то что криптография – это практическое применение математики, для понимания ее основ читателям вовсе не обязательно становиться диванными алгебраистами. Математики, лежащей в основе шифрования, не так уж много в этой книге. Примерно так же люди учатся водить машину, не интересуясь, как происходит впрыск топлива.

Кроме того, несмотря на захватывающее прошлое криптографии и даже ее военный «опыт», это не учебник истории. То, как шифрование использовалось в разные времена, прекрасно освещает другая литература[29]. Мы же сосредоточимся на современном положении вещей, обращаясь к историческим примерам только тогда, когда это уместно.

Эта книга также не о головоломках[30]. Одно из «лиц» криптографии – создание «задач», которые нужно «решить», и во время Второй мировой британское правительство действительно набирало стажеров-криптографов среди тех, кто умел и любил решать кроссворды. Но все же я не последую примеру тех, кто преподносит криптографию как искусство в первую очередь развлекательное (в конце концов, это ТЖРАЖИНПЖ ЕЖМП[31]).

В главе 2 я покажу, что такое безопасность в киберпространстве, и как криптография помогает ее обеспечить. В главе 3 я объясню разницу между ключами и алгоритмами в контексте криптографии. Затем каждой из основных криптографических функций будет посвящена отдельная глава, я имею в виду хранение секретной информации, обмен ключами, поиск и обнаружение изменений в данных и определение того, с кем мы взаимодействуем. В главе 7 мы поговорим о некорректном использовании криптографии, сосредоточившись на конкретных примерах и возможности исправить положение. Затем в главе 8 я исследую вызовы обществу, которые провоцирует использование криптографии, и политическую реакцию на них. И наконец в главе 9 я попытаюсь обрисовать будущее, которое ожидает криптографию, и поразмышлять о том, как к нему подготовиться.

Суммируя, перед вами книга о том, почему криптография важна для общества и как осведомленность о ней может нас защитить. Я хочу показать вам, что криптография в буквальном смысле ключ к киберпространству.

1. Безопасность в киберпространстве

Что означает быть защищенным в киберпространстве? Прежде чем приступать к осмыслению идеи кибербезопасности, стоит проанализировать основные элементы безопасности в реальном мире: вы увидите, что в виртуальном пространстве некоторые аспекты физической защиты отсутствуют. Сама по себе криптография заменить их не может. Ее главная задача – дать инструменты, с помощью которых можно обеспечить безопасность в киберпространстве.

Типичный день

Вы просыпаетесь утром, находите в почтовом ящике счет от своего поставщика электроэнергии и сразу же его оплачиваете. Вам нездоровится (особенно после оплаты счета), поэтому, позавтракав, вы отправляетесь в ближайшую аптеку. Короткое обсуждение симптомов с фармацевтом – и вот вы уже получили консультацию, оплатили лекарства наличными и возвращаетесь домой. А после обеда вы уже на пути к выздоровлению.

Это короткий фрагмент обычного дня в *реальном мире*, в котором мы живем. Этот мир состоит из материальных объектов и физического взаимодействия, которое зачастую «привязано» к определенному географическому положению. Давайте для начала посмотрим, насколько *безопасен* этот мир: насколько хорошо он защищен от того, что может причинить нам вред?

Для тех из нас, кому посчастливилось жить в относительно мирном и благополучном месте, почти любой день обходится без происшествий. Каждый день мы читаем и слышим в новостях о тревожных случаях, но, как правило, эти случаи исключительны, потому и попадают в новости. Мы достаточно неплохо защищены в реальном мире, так что стоит выделить элементы нашего окружения, обеспечивающие эту защиту.

Давайте подумаем о том, что *могло бы* произойти за такой же типичный день. Это упражнение потребует от нас крайне

пессимистичного мышления, граничащего с паранойей, но именно анализ того, что могло бы пойти не так, позволяет формировать механизмы безопасности. Надеюсь, этот мысленный эксперимент не отобьет у вас желание подниматься с кровати по утрам!

Нетипичный день

Вы просыпаетесь утром и находите в почтовом ящике счет – точь-в-точь один из обычных счетов за электричество. Недолго думая, вы его оплачиваете. Но этот счет на самом деле послал злоумышленник, зарящийся на ваши деньги. Вам нездоровится (и вы бы чувствовали себя еще хуже, знай вы о допущенной оплошности), поэтому после завтрака отправляетесь в аптеку, закрыв, разумеется, дверь на замок. Как только вы уходите, в ваше жилище вламывается вор. Тем временем вы садитесь в автобус, который, к несчастью, только что угнали. Каким-то чудом вам удается выбраться из автобуса и добраться до вашей цели, и вы наконец обсуждаете симптомы с человеком в белом халате. Это должен быть фармацевт, но на самом деле это психопат, находящийся в розыске, и он выписывает вам какую-то отраву. Каждому следующему покупателю этот самозванец рассказывает о вашем плохом самочувствии, и уже через несколько часов весь город знает, что вы ужасно больны. Вы платите наличными, но вдобавок ко всем своим злоключениям получаете сдачу поддельными купюрами. Вы возвращаетесь в свое недавно ограбленное жилище с опасными лекарствами. Конец.

История, конечно, совершенно нелепая. Но что интересно, каждую отдельную параноидную ее часть кто-то когда-то как минимум замышлял, поскольку в реальном мире существуют способы предотвращения большинства этих неприятностей. «Типичность» первого дня и «нетипичность» второго объясняются тремя факторами, каждый из которых заслуживает внимания: механизмами безопасности, контекстом безопасности и вероятностью возникновения угрозы.

Реальные угрозы

Для обеспечения безопасности используется множество инструментов и методик, которые я обобщенно называю *механизмами безопасности*. Давайте проанализируем те из них, которые действуют на протяжении вашего типичного дня.

Почтовые ящики бывают разными. Одни защищают только от плохой погоды, другие запираются на замок и не открываются без ключа, а в некоторых домах почтовый ящик и вовсе заменяет щель в парадной двери. Письма, которые просовываются через эту щель, защищены дверным замком, но совершенно беззащитны перед внутренними угрозами (например, интересом вашей собаки).

В ваш почтовый ящик опустили письмо в конверте. Содержимое конверта в какой-то степени защищено от случайных повреждений при доставке и от прочтения посторонними. Но эта защита довольно слаба: бумага конверта тонка, легко рвется, да и открыть его несложно. Пожалуй, самый важный элемент защиты конверта – то, что его обычно нельзя открыть, не повредив. Если не соблюдать крайнюю осторожность, получатель заметит вмешательство.

Письмо, которое вы получили, было послано от имени крупной организации, ее знакомый логотип несли на себе как сам конверт, так и его содержимое. Письмо имело характерный вид: дизайн бланка, общую структуру, шрифты, стиль речи. Все эти свойства в той или иной степени являются механизмами безопасности.

Ваша дверь была защищена замком. Современные дома иногда уже могут быть оснащены электронными системами контроля доступа, но большинство дверей запираются механически. Некоторые замки нужно закрывать ключом, другие закрываются сами, стоит захлопнуть дверь. Позже вы увидите, что с точки зрения криптографии различия между этими двумя типами замков произвели революцию.

Автобус, на который вы сели, был оформлен в знакомом фирменном стиле, на табло или на табличке значился нужный вам номер маршрута. У водителя был бейдж определенного дизайна с именем, фотографией и официальным логотипом. Вероятно даже, что водитель был одет в униформу транспортной компании и имел при себе ключи.

Фармацевт, разумеется, тоже носил официальный именной бейдж. Но вы, скорее всего, знали его в лицо: это ближайшая к вашему дому аптека, вы не раз и не два бывали здесь. Лицо и голос фармацевта – тоже механизмы безопасности. Вы разговаривали на некотором

расстоянии от других покупателей и, если не хотели, чтобы вас слышали, понизили голос. Лекарства были в запечатанной фирменной упаковке с информативной надписью и, возможно, печатью самой аптеки.

Наконец, вы платили наличными. На монетах есть надписи, насечки и чеканки, которые сложно подделать. Для купюр существует более сотни механизмов защиты, включая водяные знаки, голограммы и металлографию. Но многим проще всего определять подлинность денег на ощупь, на вид и на звук[32].

Материальный мир полон механизмов безопасности, каждый из которых защищает определенные объекты от конкретных угроз.

Контекст безопасности

Важность *контекста безопасности* в реальном мире не так очевидна. Под этой формулировкой я понимаю окружение, в котором происходят события и с учетом которого мы анализируем и интерпретируем их безопасность. Контекст – это все то, на чем мы обычно не заостряем внимание. Его роль в нашей повседневной безопасности почти незаметна, но огромна: сосредоточившись на контексте, вы сразу заметите, насколько он информативен.

Вернемся к типичному дню. Письмо в почтовом ящике было отправлено организацией, счет на оплату услуг которой вы ожидали получить: эта компания присылает вам счета за эти услуги примерно в одни и те же даты каждого месяца. Если бы счет за электричество пришел через неделю после оплаты предыдущего, вы могли бы что-то заподозрить. Сумма к оплате тоже информативна, поскольку ее можно интерпретировать в более широком контексте обычного для вас расхода электроэнергии. Она могла бы, наверное, вас удивить, но, скорее всего, не слишком сильно разошлась с вашими ожиданиями.

У автобуса на любом маршруте есть установленное расписание, поэтому, когда к остановке вовремя подъехал автобус обычного вида, сомневаться в его подлинности не было причин. Если бы он сильно опоздал, двигался рывками, или если бы водитель пребывал в прострации, у вас наверняка возникли бы опасения.

За прилавком в аптеке стоял человек, который не только выглядел, но и – что важнее – вел себя как фармацевт. Он профессионально отреагировал на ваши жалобы, со знанием дела обсудил с вами лечение. И вас, конечно, могло бы насторожить, если бы фармацевт постоянно ухмылялся или растерялся при поиске медикаментов[33].

Даже у денег есть контекст. Если вам случалось платить крупной купюрой, чей номинал во много раз превышал стоимость покупки, фармацевт мог засомневаться и проверить подлинность ваших денег.

Контекст безопасности в материальном мире по-настоящему важен. Кто не слышал фразы вроде: «Если вы видите что-то подозрительное, пожалуйста, обратитесь к сотруднику компании»? Фактически все эти фразы нам говорят: «Если вы видите что-то вне контекста, пожалуйста, поднимите тревогу».

Какова вероятность?

В оценку безопасности обязательно входит и оценка вероятности перехода потенциальной угрозы в реальную. Обычно невозможно вычислить с точностью шанс какого-то неприятного события, но на протяжении жизни мы вырабатываем интуитивное представление о реалистичности многих угроз[34].

Интуитивно же мы понимаем, что «нетипичный день», описанный выше, полностью абсурден. Почему?

Существуют ли жулики, обманывающие людей для извлечения финансовой выгоды? Конечно, их полно вокруг[35]. Однако круг их потенциальных жертв очень широк, и вероятность того, что в их сети попадете именно вы, относительно невысока. Могли ли они воспользоваться счетом за электроэнергию для своего мошенничества? Конечно. Для этого им пришлось бы составить письмо, которое выглядело бы как настоящая платежка, учесть контекст расписания и суммы к оплате. Такая афера потребовала бы значительных усилий, и при этом все еще осталась бы строго индивидуальной. Все это не делает ее невозможной, но существует много более простых и надежных способов выманивания чужих денег[36].

Точно так же нельзя полностью исключать кражу со взломом, но чаще всего каждый отдельный дом даже не в самом благополучном районе остается нетронутым. Автобусы угоняют крайне редко, и еще реже серийные убийцы прикидываются фармацевтами. Все эти ужасные вещи могут случиться, но мы знаем (в основном благодаря нашему интуитивному пониманию материального мира), что, скорее всего, этого не произойдет.

Безопасность в материальном мире

Ваш нетипичный день в материальном мире выглядит как кошмарный сон, цепочка почти невероятных событий, которые становятся еще менее вероятными, если учесть сочетание механизмов и контекста безопасности. Неправдоподобность этого примера определяется тремя свойствами реального мира.

Первое – это буквально его *материальность*. Большинство механизмов безопасности, описанных ранее, полагаются на использование органов чувств. Письмо в почтовом ящике *выглядело* подлинным, вы *узнали* фармацевта, деньги казались правильными *на ощупь*. Мы полагаемся на чувственное восприятие во всех аспектах нашей жизни и с его помощью принимаем решения о безопасности. В какой-то мере в нас с самого рождения заложено понимание разных физических угроз. Например, как показывают исследования, у младенцев есть врожденный страх пауков и змей[37]. О других угрозах в материальном мире мы узнаем с возрастом. Сочетание врожденного и приобретенного дает нам возможность формировать на основе собственных ощущений понятие безопасности в окружающей нас обстановке.

Второе важное свойство материального мира – это его *знакомость*, переработанный опыт жизни в нем. Это не означает, что мы понимаем все его аспекты, но мы привыкли ориентироваться в ситуациях, в которых оказываемся. Мы можем не знать, как именно работает двигатель автобуса, но знаем, как он выглядит, как на него сесть, и что собой представляет обычная поездка в общественном транспорте. Многие механизмы и некоторые контексты безопасности, на которые вы полагаетесь в повседневной жизни, относятся к знакомости.

Письмо в почтовом ящике казалось подлинным, поскольку вы уже прежде видели много таких писем. Автобус казался нормальным, потому что он подъехал к знакомой вам остановке в ожидаемое время. Чувство беззащитности, которое мы часто испытываем при попадании в новую для себя ситуацию, объясняется именно ее незнакомостью. Нас настораживают незнакомцы. Если бы счет за электроэнергию пришел в конверте, подписанном от руки и с международной печатью, а деньги нужно было переводить на иностранный банковский счет, вы бы вряд ли его оплатили.

Наконец, материальному миру присуща *ситуативность*. Люди и объекты физически находятся в определенном месте в определенный момент времени, что позволяет нам судить о них в ходе принятия решений о безопасности. Даже поддельный счет все равно должен был очутиться в вашем почтовом ящике в подходящий для оплаты период. Даже угнанному автобусу пришлось бы выйти на маршрут по расписанию, а угонщику – вовремя сесть за руль. Фармацевт-психопат должен был явиться в аптеку в тот день, когда у знакомого вам фармацевта выходной. Ни одно из этих нарушений физической безопасности нельзя назвать невозможным, но ситуативность затрудняет их осуществление. Террористы, похитившие и разбившие самолеты в США 11 сентября 2001 года, не только учились пилотированию, но и должны были сесть на разные авиарейсы с примерно одинаковым временем прибытия и точками посадки недалеко друг от друга[38]. Их деяние ужасно, но ситуативные трудности, которые они преодолели для его осуществления, были экстраординарными настолько, что никто даже представить себе не мог, что угроза такого рода вообще реальна.

Мы материальные существа, привыкшие защищать себя в материальном мире. Проблема в том, что киберпространство – это нечто совершенно другое.

Кибердень

Пришло время поговорить о дне другого рода: *кибердне*.

Вы просыпаетесь утром и проверяете свою электронную почту. Среди груды спама обнаруживается уведомление о необходимости

заплатить за электроэнергию, что вы и делаете. Вам нездоровится, но благодаря прелестям киберпространства покидать дом в поисках лекарства нет нужды: вы задаете симптомы в поисковой системе, находите интернет-аптеку, заказываете медикаменты, оплачиваете их банковской картой и ждете доставки.

Или как насчет этого?

Вы просыпаетесь утром и проверяете свою электронную почту. Среди груды спама обнаруживается счет, выставленный, по всей видимости, вашим поставщиком электроэнергии. На самом же деле его послал жулик, пытающийся выманить у вас деньги, что ему и удается. Вам нездоровится, поэтому вы задаете симптомы в поисковой системе и находите сайт, предлагающий лекарства по удивительно адекватным ценам. Поисковая система делится вашими симптомами с несколькими партнерскими организациями, в числе которых оказывается ваша страховая компания, которая решает увеличить размер ваших взносов. Вы заказываете медикаменты и платите своей банковской картой. К несчастью для вас, этот «аптечный» веб-сайт размещен на компьютере в какой-то квартирке в Руритании[39] и продает продукты сомнительного качества. У этого веб-сайта есть несколько побочных «бизнес-направлений», одно из которых – быстрые покупки в сети при помощи ваших банковских реквизитов, а другое – удаленная установка на ваш компьютер пары программ, позволяющих неведомому руританцу найти на нем все, что может вызвать интерес, включая пароли и финансовые данные. Вас определенно ограбили, хотя вы даже не выходили из дома. Это был плохой кибердень.

Какой из этих двух кибердней «типичен»? Естественно надеяться, что вторая версия менее вероятна. Может быть, это даже действительно так, но для ее описания мне не потребовался полет фантазии, который лег в основу абсурдного нетипичного дня в материальном мире. Плохой кибердень выглядит правдоподобным, его элементы – обычными и распространенными. Как же так?

Провернуть мошенничество с поддельным счетом в киберпространстве намного легче, чем в реальном мире. Прежде всего, в Интернете намного дешевле и проще разослать миллионы фальшивых электронных уведомлений об оплате. Большую часть проигнорируют, но один-два успешных результата окупят всю затею. К тому же рядовому клиенту сложнее проверить подлинность цифрового

требования, так как цифровые средства связи в разнообразии форм и стилей пока уступают материальным[40].

Вводя запрос в поисковую систему, мы очень плохо представляем, что происходит с данными дальше. Они исчезают в киберпространстве, после чего компания, стоящая за поисковой системой, может обрабатывать их так, как ей вздумается (по крайней мере в теории). Когда результаты поиска выводят нас на онлайн-продавца, судить о его добропорядочности и качестве товара можно только по его сайту, тому, как он выражается, и ценам, которые он предлагает. Если мы не знакомы с этим продавцом, нам придется в какой-то степени принять его слова на веру. Большинство людей не осознают, насколько легко организовать бизнес в киберпространстве и создать настоящий (на первый взгляд) интернет-магазин из своей спальни в Руритании.

Покупки в Интернете по чужим банковским реквизитам будут продолжаться, скорее всего, пока банковская система противодействия мошенничеству не посчитает эту активность подозрительной, но это может произойти слишком поздно. Именно поэтому похищение и продажа информации о банковских картах сейчас лидирует среди преступных промыслов в киберпространстве. Удаленная установка на компьютер вредоносного ПО тоже не вызывает проблем – обычно для этого достаточно, чтобы ничего не подозревающий пользователь щелкнул по ссылке или загрузил вложенный файл. Такие вредоносные программы могут, к примеру, легко просканировать компьютер на предмет паролей и банковских реквизитов. Что еще хуже, они могут оставаться на компьютере вечно, играя роль цифровых «шпионов»[41].

Плохой кибердень гораздо, гораздо вероятней, чем описанный ранее нетипичный день в реальном мире.

Незащищенность киберпространства

Киберпространство, каким бы оно ни было и где бы оно ни находилось, кардинально отличается от материального мира, и это отличие весьма существенно для безопасности. Чтобы понять, почему обеспечение безопасности в киберпространстве сопряжено с особыми

трудностями, стоит взглянуть на него с точки зрения трех аспектов материального мира, которые мы уже обсуждали.

Прежде всего, киберпространство по своей природе не *материально*. Конечно, некоторые его элементы – вычислительные центры, компьютеры, маршрутизаторы и провода – вполне осязаемы, но информация, которая к ним относится, производится ими и обрабатывается, существует только в виртуальном мире. Информация в киберпространстве представлена только цифровыми данными. Вы не можете их пощупать или положить в конверт. Именно благодаря нематериальности цифровых данных с ними можно делать столько удивительного, в том числе копировать с идеальной точностью, преобразовывать до неузнаваемости и передавать по планете со скоростью света. Возможность представлять и использовать информацию цифровым образом оказалась по-настоящему революционной.

Ввиду нематериальности цифровых данных для их защиты подходят очень немногие механизмы безопасности из тех, что мы используем в реальном мире. Конечно, мы можем надежно хранить флеш-накопитель в ящике стола, но, как только нам становится нужна записанная на нем информация, мы должны как-то подключить его к киберпространству, и – оп! – физическая защита теряет свою эффективность. В киберпространстве необходимы совершенно другие механизмы безопасности.

Назвать киберпространство *знакомым* тоже нельзя. Не в том плане, что мы не привыкли в нем работать. В конце концов, мы зависим от поисковых систем в Интернете, продаем и покупаем онлайн, общаемся в социальных сетях. Мы все сильнее привыкаем к жизни в киберпространстве. Но знакомы ли мы с этим пространством как таковым? Многие ли из нас имеют хоть какое-то представление о том, как оно работает? Мало кто понимает, как устроены компьютеры, не говоря уже о том, как их программируют, как они соединяются и обмениваются информацией. Найти тех, кто разбирается в принципах обработки информации в киберпространстве, не проще. Куда на самом деле попадают данные, которые мы вводим? Кто их может видеть? Что с ними делают? Для большинства из нас киберпространство сродни волшебству: мы жмем кнопку – и (абракадабра!) – что-то происходит[42].

Незнакомость киберпространства несет в себе опасность, так как без элементарного понимания, что это такое и как оно работает, нам приходится слепо доверять системам, которые якобы должны делать то, что нам нужно. Это делает нас наивными и уязвимыми, что, в свою очередь, серьезно сказывается на безопасности: если что-то идет не так, мы не в состоянии это заметить. Мы даже не знаем, что в принципе может пойти не так, поскольку не знаем, чего следует ожидать. *Если вы видите что-то подозрительное, пожалуйста, обратитесь к сотруднику компании*. Это не поможет, если у вас нет ни малейшего представления о том, что подозрительно, а что нет.

Самое главное – то, что нам недостает элементарного здравого смысла, на основе которого мы принимаем решения о безопасности в материальном мире. В киберпространстве люди идут на такие риски, которые в реальной жизни были бы немыслимы, – шлют грабителям открытки, когда уезжают в отпуск (рассылая внерабочие сообщения и публикуя в Интернете свежие фотографии[43]), печатают на футболках свои банковские реквизиты (покупая еду на ненадежном веб-сайте) и ведут прямую трансляцию с домашних камер слежения (избыточно используя социальные сети). Наши предки в африканских саваннах понимали на уровне инстинктов, что при виде льва они должны что есть духу бежать к ближайшему дереву, и это мы от них унаследовали. Нам не нужно дважды думать, стоит ли, уходя из дома посреди большого города, запирать дверь на замок. Однако в киберпространстве такого здравого смысла еще очень мало. Мы не видим открытые электронные двери и уж точно не знаем, как их закрыть. Нам сложно заметить цифровых львов, даже когда они ходят туда-сюда по нашим экранам.

Наконец, киберпространство свободно от ограничений *географического положения*. Это, наверное, самое главное его преимущество. Мы можем делать покупки, общаться с друзьями, просматривать фотографии, работать и планировать путешествия в любую точку планеты, не выходя из дома. Это невероятные возможности, и, что еще удивительнее, повседневные невероятные возможности.

Тем не менее заниматься своими делами удаленно могут разные люди, в том числе и те, чьи интересы противоречат нашим. Жулик может искать и находить жертв по всему миру. Та же история с

правительствами и корпорациями, которые хотят больше знать о нашей повседневной жизни. В реальном мире угрозы в основном исходят от того, что нас окружает. В киберпространстве они приходят отовсюду.

Суть проблемы

Чтобы оценить потенциальные угрозы в киберпространстве, стоит вернуться к трем аспектам безопасности, изложенным в начале этой главы. Давайте рассмотрим их в обратном порядке.

Во-первых, многие потенциальные угрозы имеют намного более высокую вероятность возникновения в киберпространстве, чем в материальном мире[44]. Обычный человек, занимающийся своими делами, как правило, не становится жертвой руританских мошенников. О киберпространстве этого сказать нельзя. Не каждое даже супертоталитарное государство постоянно отслеживает повседневную жизнь своих граждан чисто материальными средствами, такими как развитая сеть информаторов[45]. В киберпространстве это становится делать все проще, и люди об этом даже не подозревают[46].

Во-вторых, в киберпространстве ослабевает наша способность учитывать контекст в принятии решений о безопасности. Стоит ли доверять тому или другому сайту? Ответить на этот вопрос почти всегда непросто. Мы редко сталкиваемся с такими трудностями в материальном мире, где внешний вид и атмосфера помещения становится источником контекстной информации о магазине. Если кто-то постучит вам в дверь и начнет расспрашивать о вашем банковском счете, вы вряд ли поддадитесь. Но мало кого настораживает электронное письмо с похожими вопросами якобы от своего банка. Лишенные защиты, которую дает физический контекст, мы хуже анализируем угрозы безопасности.

Наконец, базовые защитные механизмы, вокруг которых мы выстраиваем безопасность в материальном мире, не подходят для киберпространства. Мы не можем «прошептать» электронное письмо, заклеить воском цифровой документ или узнать в лицо продавца за прилавком интернет-магазина.

Киберпространство сделало мир меньше, из-за чего многие потенциальные угрозы стали ближе. Киберпространство – это место, которое большинство из нас совершенно не понимает. Что еще хуже, в нем невозможно использовать традиционные средства безопасности. Похоже, у нас возникла проблема.

На помощь приходит криптография

Я обрисовал мрачные перспективы и потенциал безопасности в киберпространстве. Угрозы и вправду реальны, а обеспечение защиты связано с существенными трудностями. Но ведь мы каждый день пользуемся Интернетом без особых проблем. Неужели это простое везение?

Было бы ошибкой полагать, что понятие безопасности в киберпространстве отсутствует. Специалисты осознают многие виртуальные угрозы, и огромная часть технологий была разработана сразу с расчетом на определенный уровень защиты. Положение вещей нельзя назвать идеальным, но «идеальной» безопасности не существует ни в киберпространстве, ни в реальном мире.

Главная идея состоит в том, что любые концепции безопасности в киберпространстве должны быть основаны на фундаментальных защитных механизмах, рассчитанных на цифровую информацию. Если нам удастся соорудить эффективные механизмы цифровой безопасности, способные заменить замки, печати и распознавание лиц, мы сможем интегрировать их в широкий круг систем и процессов, которые будут защищать нас в киберпространстве. В идеале эти инструменты должны имитировать уровень безопасности, доступный нам в материальном мире. А если повезет, киберзащиты время от времени будут становиться еще надежнее.

В этом фактически и состоит ключевая роль криптографии. Она предоставляет пакет (или, если хотите, набор) механизмов безопасности, которые можно развернуть в киберпространстве. Каждый из этих криптографических инструментов по отдельности довольно прост и позволяет выполнять такие важные задачи, как сокрытие цифровой информации от чужих глаз, обнаружение изменений, внесенных в электронный документ, или идентификация

компьютера. Однако хорошо продуманное сочетание этих механизмов позволяет создавать чрезвычайно сложные системы безопасности, необходимые, к примеру, для поддержки безопасных финансовых транзакций, защиты электронных сетей распределения электроэнергии или проведения выборов в Интернете.

Сама по себе криптография не делает и не может сделать киберпространство безопасным, у этого процесса слишком много разных аспектов, чтобы ограничиваться только ее механизмами. Но, хотя безопасность дома нельзя свести к замкам на дверях, сложно себе представить дом вообще без замков. Точно так же одной лишь криптографии недостаточно для защиты банковских сетей, но без нее глобальная финансовая система точно бы не выжила[47].

2. Ключи и алгоритмы

Криптография предоставляет механизмы, необходимые для безопасной работы в киберпространстве. Прежде чем исследовать их возможности, нужно разобраться в том, как они устроены. Весь фундамент, на который опирается криптография, состоит из двух главных компонентов: *ключей* и *алгоритмов*.

Важнейшая роль ключей

Давайте еще раз проанализируем ваш типичный день в материальном мире и подумаем о назначении некоторых механизмов безопасности, которые в нем фигурируют.

Конверт нужен для того, чтобы *только* энергетической компании были известны подробности отправленного вам счета. Замок на двери нужен, чтобы *только* вы могли войти в свой дом. Поведение человека за прилавком аптеки характерно *только* для настоящего фармацевта. Детали приглушенного разговора с фармацевтом были слышны *только* вам двоим. Физические свойства денег имеют *только* настоящие купюры и монеты.

Только, только… суть любого механизма безопасности в том, чтобы те или иные вещи могли происходить *только* в определенных обстоятельствах. Механизм безопасности можно использовать, чтобы отмежевать себя от других или выделить один из множества элементов. Он дает нам *особую* возможность. Ключ и замок дают возможность открыть дверь и войти в свой дом. Разговор шепотом дает возможность исключить из него тех, кто находится за пределами слышимости. Защитные элементы купюры позволяют использовать ее в качестве законного платежного средства.

В материальном мире возможности безопасности обеспечиваются разными средствами. Самое очевидное – *что-то, чем вы располагаете*: ключ, бейдж, билет, рекомендательное письмо[48]. Или *то, где вы находитесь* – достаточно близко, чтобы расслышать личный разговор, или внутри концертного зала, где проходит мероприятие, на

которое вы купили билет. Или *что-то, что вам известно* – голос друга или то, что для входа в пещеру с сокровищами нужно произнести: «Сим-сим, откройся»[49]. Или даже *то, кем вы являетесь*, как в случае со сканированием отпечатков пальцев или радужки глаза. И, конечно же, особая возможность может обеспечиваться сочетанием подходов. У вашего фармацевта могло быть что-то особенное (бейдж), он мог стоять в особенном месте (за прилавком аптеки), быть кем-то особенным (тем, кого вы раньше видели) или знать что-то особенное (фармакология и порядок назначения лекарств).

Этот последний способ предоставления особых защитных возможностей – что-то, что вам известно – легче всего адаптировать к киберпространству. В криптографии эта особая информация зовется *ключом*. Термин выбран не случайно: криптографический ключ играет примерно ту же роль, что и дверной. Только тот, кто его знает, может выполнить определенное действие – по аналогии с тем, как открыть дверь в конкретном доме может только обладатель подходящего ключа. В большинстве случаев ключ представляет собой секретный фрагмент информации, знание которого используется в киберпространстве для отличения одного человека от другого. Заметьте, я применил выражение «в большинстве случаев». Пока что предположим, что ключи являются секретной информацией, хотя это не всегда так.

Должен признаться, что выше я выразился не совсем точно. В большинстве случаев взаимодействуют в киберпространстве *компьютеры*, а не люди; больше того, иногда люди вовсе не принимают активного участия в работе этих компьютеров. Ранее я говорил, что «знание» ключа позволяет отличить одного «человека» от другого; но было бы правильней сказать, что только *сущность* (человек или компьютер) с *доступом* к ключу может выполнять определенные действия в киберпространстве.

Самое важное свойство ключа, которое необходимо понимать, состоит в том, что особая возможность входить в дом принадлежит не лично вам, а любому, у кого есть дубликат ключа от вашей двери. То же самое относится и к криптографии. Доступа к подходящему криптографическому ключу достаточно для того, чтобы платить за сотовую связь со счета, делать покупки с помощью банковской карты, загружать фильмы, открывать двери автомобиля и т. д.

Биты и байты

Мы пользуемся криптографией ежедневно и в большинстве случаев с применением ключей. Зачастую это происходит неосознанно, но давайте все же поговорим о том, как выглядят криптографические ключи.

Для начала вспомним, как компьютеры представляют информацию. Когда компьютер получает данные, он переводит их в числа, точно так же, как наш мозг превращает увиденное или услышанное в символы языка. Вся компьютерная информация, которую мы храним, передаем и обрабатываем, таким образом, является числовой. Когда мы набираем текст на клавиатуре, компьютер переводит его в цифровые коды и только потом делает с ним то, на что ему дана команда. Когда мы хотим получить информацию назад, компьютер преобразует эти числа в понятный нам текст. Аналогичный процесс происходит, когда мы загружаем на сервер изображения: они состоят из крошечных пикселей, каждый из которых компьютер превращает в число, обозначающее конкретный цвет.

Дальше – сложнее. Компьютер работает не в привычной нам десятичной системе счисления, а в *двоичной*, состоящей только из нолей и единиц. Звучит страшнее, чем на самом деле: это всего лишь еще один способ записи чисел, у каждого десятичного числа есть двоичное представление и наоборот. Например, десятичное число 17 записывается как 10001 («один ноль ноль ноль один», а не «десять тысяч один») в двоичной системе, а двоичное число 1101 – как 13 в десятичной. Каждую цифру двоичного кода называют *битом*, и эти биты формируют неделимые единицы числовой информации. Четыре бита составляют *ниббл* (от англ. nibble – покусывать), а два ниббла – *байт* (от англ. byte – кусать; и не говорите больше, что у компьютерщиков нет чувства юмора!).

Как правило, информация, которую мы хотим обработать на компьютере, состоит не только из чисел. Допустим, вы набрали на клавиатуре символы «K9!». Прежде чем сделать что-то с этими данными, компьютер должен представить их в двоичном виде. Клавиатурные символы преобразуются в биты по системе, известной как ASCII (American Standard Code for Information Interchange), которая

описывает правила сопоставления кнопок клавиатуры и битов. В нашем примере символу «K» по ASCII соответствует байт 01001011, символу «9» – 00111001[50], а для «!» это будет 00100001. Таким образом компьютер, получивший код ASCII 01001011 00111001 00100001, знает, что для представления пользователю его следует перевести обратно в строку «K9!».

Полезно вспомнить и о размере данных. Поскольку они состоят из двоичных чисел, измерять их проще всего в количестве бит или байтах. Например, число 1011001100001111 имеет длину 16 бит или 2 байта. Для больших данных используются более грандиозные термины, такие как *килобайты* (1000 байт), *мегабайты* (1000 килобайт), *гигабайты* (1000 мегабайт) и *терабайты* (1000 гигабайт).

Криптографические ключи – это лишь особые элементы данных, поэтому компьютер их тоже должен представлять в виде двоичных чисел. А поскольку размер ключа – одна из важных мер безопасности, упоминания о *длине ключей*[51] в криптографических алгоритмах нередки. В современной криптографии ключ, как правило, имеет длину 128 бит.

Где мой ключ?

Если постоянно пользоваться криптографическими ключами, возникает вопрос: где они находятся?

Рассмотрим конкретный пример. Каждый раз, когда вы звоните кому-то по сотовому телефону, вы используете криптографию. Безопасность этого процесса опирается на способность сотового оператора отличить вас от остальных 5 миллиардов абонентов на планете[52]. Для этого оператор выдает вам секретный криптографический ключ – число, «известное» *только* ему и вам, при помощи которого вы сообщаете оператору о попытке сделать звонок. А теперь я объясню, почему это *почти* соответствует действительности.

Что это за особое секретное число, которое используется для звонка? Это явно не ваш телефонный номер – он не секретный. Криптографический ключ мобильного телефона вам наверняка

неизвестен. И тому есть две веские причины, ни одна из которых не сводится к тому, что вам этот ключ знать нельзя.

Первая и, наверное, главная причина в том, что криптографические ключи представляют собой *большие* числа. Если вас попросят запомнить число от 0 до 10, вы легко с этим справитесь. Скорее всего, вы способны запомнить числа до 10 000 или даже до миллиона, так как числа такой длины часто используют в качестве PIN-кодов (хотя об этом чуть позже). Но в криптографических масштабах 1 миллион – это *не* большое число. Ключи не просто очень большие, их размер едва ли не за гранью нашего понимания.

В порядке упражнения попытайтесь представить себе количество звезд во вселенной, умноженное на 40 000[53]. Даже если вам удастся это вообразить, вы все равно будете оперировать значениями не того масштаба. Ключи примерно такого размера когда-то действительно использовались, но их давно уже не признают достаточно безопасными в большинстве современных сфер применения криптографии. Теперь мы пользуемся ключами в триллион раз большими. Если у вас от таких чисел начала кружиться голова, то вы уловили суть. Обычный человек не в состоянии запомнить современный криптографический ключ.

Сотового оператора не интересует, кто говорит по телефону и даже с какого аппарата прошел звонок. Оператора заботит, куда послать счет за услуги. Это вторая причина, почему вам неизвестен ключ, который используется в вашем сотовом. Таким образом, оператору нужен какой-то уникальный аспект вашей мобильной учетной записи, которым может быть невообразимо большое число. Именно его вы и получаете при регистрации номера. Это очень маленькая пластиковая карта с крошечным встроенным микрочипом, так называемым *модулем идентификации абонента* (англ. subscriber identity module – SIM), которая вставляется в ваш телефон. Основное назначение SIM-карты состоит в хранении криптографического ключа. Этот ключ позволяет отличить вашу учетную запись от любой другой на планете, поэтому, если вы одолжите кому-то свой телефон или вставите свою SIM-карту в другое устройство, счет придет именно вам.

Итак, криптографические ключи в большинстве своем являются огромными числами, пользуются которыми непосредственно компьютеры, а не люди. Поэтому большинство ключей находится либо

на самих компьютерах, либо на устройствах, которые к ним подключаются. Например, ключи для защиты банковских транзакций хранятся на чипе, встроенном в вашу платежную карту. Ключи к вашей сети Wi-Fi – в вашем маршрутизаторе. Ключи для защиты данных, которыми вы обмениваетесь с интернет-магазином, зашиты в программный код вашего браузера. Криптографический ключ, позволяющий вашей машине открывать дверной замок, когда вы к ней приближаетесь, находятся в брелоке (и пусть вас не вводят в заблуждение слова о так называемой технологии входа «без ключа»: на самом деле ключ здесь двойной, одна его часть физическая, а другая криптографическая). Вы не знаете, какое число представляет любой из этих ключей, но у вас есть доступ к местам, где они хранятся.

Когда секретная информация не является ключом

Итак, криптографические ключи – это секретная информация, знание которой можно использовать для идентификации той или иной сущности в киберпространстве. Но что насчет таких секретных данных, как пароли и PIN-коды[54]? Можно ли их считать криптографическими ключами?

Не совсем, хотя иногда они таковыми оказываются. В каком-то смысле. Запутались? Неудивительно, различие между этими понятиями и правда тонкое.

Криптографические ключи действительно чем-то похожи на пароли и PIN-коды, но знак равенства между ними поставить нельзя. Пароли и PIN-коды, несомненно, являются секретными данными, необходимыми для обеспечения безопасности в киберпространстве. Но считать ли их криптографическими ключами, зависит от способа применения.

Пароли и PIN-коды в основном применяются для идентификации. Например, когда вы входите в систему, компьютер запрашивает пароль и проверяет его корректность. Если проверка прошла успешно, компьютер выводит на экран приветствие. С точки зрения криптографии в этом нет ничего особенного, так как в основе этого процесса нет шифрования[55]: вы всего лишь предоставляете пароль, чтобы компьютер мог его проверить.

Именно в этом и состоит ключевая проблема входа в систему. Пароль – это секретные данные, которые вам полагается оберегать, но, входя в систему, вы их «выдаете». В каком-то смысле вы теряете контроль, поскольку вам приходится доверять устройству, которому вы передаете их, а заодно всем сетям и устройствам, которым эти данные переправляются далее. Вы вынуждены верить, что все они не допустят никаких злоупотреблений.

Ввод пароля в домашний компьютер вряд ли покажется вам чем-то безрассудным, и вы, конечно же, правы. Но иногда мы взаимодействуем с удаленными компьютерами, например когда вводим пароль для доступа к каким-то ресурсам на веб-странице. В этом случае пароль передается незащищенным по компьютерным сетям, прежде чем дойдет до сервера, на котором физически находится сайт (некоторые хорошо спроектированные веб-сайты используют для защиты паролей криптографию, но не все). Любой, у кого есть доступ к промежуточной сети, сможет прочитать ваш пароль и позже использовать его, чтобы выдать себя за вас. Точно так же, снимая деньги в банкомате, мы «выдаем» свой PIN-код, и важные секретные данные передаются другому устройству[56].

Криптографические ключи ни в коем случае нельзя так раскрывать. Их *используют* для демонстрации того, что они вам известны, но сами ключи при этом не раскрываются. Таким образом ключ остается секретным на протяжении всего процесса – как до, так и после использования. Этот уровень секретности имеет куда более строгие требования по сравнению с теми, которые мы предъявляем к паролям и PIN-кодам.

Но иногда криптографические ключи напрямую связывают с паролями: для простоты использования. Как вы помните, они представляют собой огромные числа, запомнить которые нереально. В связи с этим они обычно хранятся на устройствах. Но это не всегда представляется возможным.

Допустим, вы решили скрыть содержимое отдельного конфиденциального файла на своем компьютере с помощью криптографии. Предположим, вы нечасто этим занимаетесь, поэтому в вашей системе не включено автоматическое шифрование файлов (между прочим, вы можете его включить). Таким образом вам

придется создать ключ специально для этого случая, который придется как-то запомнить на будущее.

Один из методов запоминания огромных криптографических ключей состоит в том, чтобы вычислять их *из* паролей. Иными словами, вначале мы выбираем пароль, который компьютер преобразует в число (для этого существуют стандартные процедуры). Дальше это число претерпевает развертывание в намного большее значение (это тоже делается по стандартным алгоритмам), которое можно будет использовать в качестве криптографического ключа. Каждый раз, когда нам нужен этот ключ, мы можем просто вспомнить пароль и вычислить его заново. Сам пароль при этом является не ключом, а его отправной точкой, начальным значением (англ. seed – семя), из которого этот ключ «вырастает»[57].

Пароли и PIN-коды – секретная информация, которую можно запомнить. Это их определяющее свойство, которое в равной мере можно считать важнейшим преимуществом и фундаментальным недостатком. Многие люди выбирают в качестве паролей обычные слова. Двадцать томов Оксфордского словаря английского языка содержат примерно 300 000 слов[58]. В качестве секретных данных пароли и PIN-коды обладают относительно невысоким уровнем защиты, поскольку количество возможных вариантов не слишком-то велико. Это ограничение подчеркивает одно из отличий между «простыми» секретными данными, такими как пароли и PIN-коды, и криптографическими ключами: если вы способны запомнить фрагмент информации, он недостаточно велик для того, чтобы быть хорошим криптографическим ключом.

Рецепты безопасности

Криптографические ключи – это секретные данные, которые никогда не «выдаются», а только «используются». Как же это происходит?

Вернемся к механизмам безопасности материального мира. Здесь напрашивается аналогия с дверным замком, в которой фигурирует физический ключ. Предположим, что у вас на двери установлен традиционный замок без какой-либо электронной магии (если у вас

цифровой замок, вы практически наверняка открываете свою дверь с помощью криптографии). Чтобы открыть дверь, ключ недостаточно показать. Вы должны вставить его в замочную скважину, повернуть и, если все прошло удачно, войти. Что именно при этом происходит, зависит от типа вашего замка.

Замочный механизм – штука очень точная, но почти невидимая. Например, когда вы поворачиваете ключ по часовой стрелке, он в определенном порядке нажимает внутри замка несколько цилиндров, которые вращают рычаг и, если все правильно настроено, открывают затвор, который физически запирает дверь. Здесь важен тот факт, что в цепочке событий участвует ключ. Если ключ подходит, замок открывается. Если же вставить неправильный ключ, он не сможет открыть затвор, и дверь останется запертой.

Самого наличия физического ключа недостаточно. Ключ должен быть интегрирован в процесс, который в конечном счете приводит к открытию замка. Этот процесс состоит из последовательности отдельных, но точных действий, которые в совокупности отпирают затвор. Выполнено должно быть *каждое* из этих действий, иначе войти не удастся. Если вставить ключ в замок не до конца, или повернуть его не в том направлении, или если хотя бы один из металлических цилиндров внутри замка не нажат, процесс не увенчается удачей. Больше того, эти действия должны быть выполнены в *правильном порядке*. Цилиндры не откроют затвор, если ключ не был повернут, а повернуть его можно только после того, как он вставлен в замок.

Обратите внимание: ключ от двери и процесс открытия играют отдельные роли в защите вашего дома. Процесс открытия во многом стандартизован, все замки одной модели открываются одинаково. А вот дверной ключ уникален, у всех замков одной модели должны быть разные ключи.

Поскольку криптографические ключи – это числа, любой процесс, в котором они используются, неизбежно состоит из последовательности математических операций, таких как сложение, умножение, перемешивание или перестановка. Такой вычислительный процесс я далее называю *алгоритмом*. В сущности, это просто рецепт, содержащий набор действий-ингредиентов и порядок их выполнения.

Сделай то, сделай это, затем то, затем это и т. д. и т. п. Число, которое мы получаем в результате, называется *выводом* алгоритма.

Получение корректного вывода зависит от успешного выполнения каждого шага алгоритма в предусмотренном порядке.

Чтобы приготовить ужин по рецепту, вам понадобятся все ингредиенты. Алгоритм работает похожим образом: вы не получите вывод, пока не подадите что-то на вход. Конкретный *ввод* алгоритма зависит от того, для каких задач этот алгоритм был создан. У большинства криптографических алгоритмов ввод состоит из данных, которые нужно защитить, и криптографического ключа.

Основная идея заключается в том, что криптографический алгоритм создается общим для всех пользователей системы (например, он может быть реализован на каждом мобильном телефоне, подключенном к сети), но каждый пользователь обладает уникальным ключом. Мы вводим данные и свой ключ в криптографический алгоритм, который затем вычисляет на их основе вывод (и любые изменения данных или ключа приведут к получению другого вывода). Этот вывод представляет собой значение, которое необязательно скрывать (например, его можно передавать по беспроводной сети в ходе телефонного звонка). Он свидетельствует о том, что тот, кто его вычислил, сумел ввести в алгоритм ключ пользователя. При этом сам ключ не раскрывается. Это краткое описание того, как обычно работает шифрование. В следующих главах я покажу, как с помощью этого процесса можно обеспечивать целый спектр разных аспектов безопасности.

Числовые миксеры

Алгоритмы – это рецепты, а ключи – особые и чаще всего секретные ингредиенты. Поскольку вывод криптографического алгоритма путешествует по киберпространству без какой-либо защиты, мы должны позаботиться о том, чтобы тот, кто его прочитает, не смог получить из него ключ. Иными словами, мы с радостью дадим отведать результаты нашей готовки, но не хотим, чтобы кто-нибудь смог определить ингредиенты.

Если просто высыпать все на сковороду и обжарить, возникнет проблема: ингредиенты, несмотря на перемешивание, почти не изменяются. Нам нужно, чтобы криптографический алгоритм уничтожил все признаки исходного ввода. Возможно, более подходящей аналогией будет фруктовый коктейль, ингредиенты которого измельчаются настолько сильно, что от их первоначального вида почти ничего не остается (хотя иногда подсказкой может служить цвет коктейля). Мы хотим перемешать входные значения настолько эффективно, чтобы вывод не содержал никаких признаков того, какими они были. Хороший криптографический алгоритм должен выдавать однородный и бесцветный коктейль.

Цифровым эквивалентом «однородности и бесцветности» является *случайность*. Этому понятию на удивление сложно дать формальное определение, поэтому я не стану вникать в подробности[59]. Тем не менее ваше интуитивное понимание случайности наверняка в целом верно. Суть случайности в непредсказуемости. У случайно сгенерированных чисел нет очевидных закономерностей. Что важно, связь между случайностью и непредсказуемостью чисел должна сохраняться *на протяжении большого количества повторений*. Например, если вы подбросите монету пять раз и во всех случаях выпадет орел, результат не покажется вам случайным. Вы можете даже подумать, что монета нарочно разбалансирована. Но, если выпадет орел, решка, орел, орел, решка, в случайности результата не будет сомнений.

На самом же деле эти два исхода одинаково вероятны (если предположить, что монета сбалансирована); шансы на получение каждого из них составляют один к тридцати двум. Настоящей странностью было бы получать пять орлов (или те же орел, решку, орел, орел, решку) при каждых пяти подбрасываниях. На самом деле, если вы будете подбрасывать монету достаточно долго, и на протяжении эксперимента *любая* последовательность орел-решка будет выпадать заметно чаще, чем один раз из тридцати двух, это означает, что процесс не случайный. Если монета сбалансирована, то для каждой новой серии из пяти подбрасываний ни один исход не окажется вероятнее другого.

Понятие случайности тесно связано с криптографией в двух важных аспектах. Во-первых, секретные криптографические ключи должны

генерироваться случайно. В противном случае некоторые из них будут генерироваться с большей вероятностью, чем другие, что поможет тем, кто пытается их подобрать. Именно случайность в сочетании с большой длиной настолько затрудняет угадывание и запоминание криптографических ключей. С другой стороны, пароли редко бывают случайными, поскольку они составлены из запоминающихся слов (например, *BatMan1988* или даже *B@tM@n1988*) намного чаще, чем из бессмысленных сочетаний символов вроде *8zuHmcA4&$*. Из-за краткости и недостатка случайности пароли намного уступают криптографическим ключам в плане обеспечения безопасности.

Второй, не менее важный аспект состоит в том, что хороший криптографический алгоритм должен вести себя, словно генератор случайных чисел[60]. Если вы шифруете какие-то данные, результат должен выглядеть «бессмысленным» и не включать значимых закономерностей. Эту случайную, на первый взгляд, информацию можно послать через Интернет, и любой посторонний наблюдатель увидит лишь облако нолей и единиц.

Процесс смешивания, необходимый для защиты нашей деятельности в киберпространстве, еще более требователен. Представьте, что у шеф-повара есть рецепт бесцветного и однородного фруктового коктейля (это лишь аналогия, не судите строго). Он неплох на вкус и перемешан настолько хорошо, что от каждого отдельного ингредиента не осталось и следа. Теперь представьте, что шеф-повар перечисляет вам ингредиенты и тайно готовит новый коктейль, самую малость изменив рецепт (например, чуть больше моркови и меньше яблок). Вы снова пробуете. Тоже неплохо; в общем-то вкус почти такой же, как у предыдущего. А теперь шеф-повар предлагает вам назвать ингредиенты во втором коктейле.

Разумно предположить, что рецепты почти не различаются. Вы можете немного ошибаться, но такой ответ будет близок к истине. Знание состава первого коктейля действительно поможет при вычислении ингредиентов второго. Однако в криптографии такого рода связь очень нежелательна, и аналогия теряет свою наглядность.

Представьте, к примеру, что криптографический алгоритм используется для шифрования похожих балансов на двух банковских счетах. Мы не хотим, чтобы владелец одного счета смог догадаться о балансе другого по их внешнему сходству. Таким образом хороший

криптографический алгоритм будет эквивалентом рецепта, настолько чувствительного к ингредиентам, что даже малейшее изменение (один кусочек моркови вместо одного кусочка яблока) приведет к радикальному изменению вкуса коктейля. Иными словами, небольшое изменение ввода криптографического алгоритма должно вызывать непредсказуемые изменения в его выводе. Следовательно, если одному и тому же криптографическому алгоритму подать на вход два почти одинаковых ключа или банковских баланса, должны получиться два никак не связанных между собой вывода. Тот, кто на них посмотрит, не получит ни малейшего представления о том, что два исходных ключа или баланса почти одинаковы.

На этом мы пока что завершим тему перемешивания. Сейчас вам достаточно понимать, что хорошие криптографические алгоритмы не позволяют установить связь между вводом и выводом без знания ключа[61].

Лучшие повара и секретные рецепты

Получить сносный ужин, поджарив накрошенные продукты на сковороде, довольно легко. Но составить рецепт, который удивит кулинарных критиков – совсем другое дело. В высокой кулинарии созданием рецептов занимаются лучшие повара.

В криптографии все обстоит похожим образом. Алгоритм, который, на первый взгляд, работает хорошо, но на самом деле небезопасен, создать легко, тогда как разработка хороших криптографических алгоритмов, которые выдерживают проверку временем, чрезвычайно сложна. К сожалению, некоторые создатели новых технологий предпочитают собирать криптографические алгоритмы на коленке. Уязвимости таких самоделок обычно обнаруживаются уже в первые месяцы после развертывания и порой оборачиваются катастрофой для разработок, которые их используют[62]. Создание криптографических алгоритмов, пригодных для широкого применения в современных условиях, требует изрядного опыта и умений.

Но допустим, вы уже тщательно спроектировали хороший криптографический алгоритм. Какую информацию о нем стоит

раскрывать? В конце концов, выдающийся шеф-повар вполне может хранить свои лучшие рецепты в тайне.

В пользу секретности криптографических алгоритмов можно привести как минимум один довод. Представьте, что хакер взломал компьютерную систему и обнаружил базу данных, содержимое которой зашифровано. Ему нужно подобрать секретный ключ. Если в системе использовался хороший криптографический алгоритм, получить ключ из одной только базы данных невозможно. Но знание алгоритма уже может послужить отправной точкой для попытки угадать ключ и расшифровать БД. Шанс на то, что ему повезет, невелик, но он существует. В то же время хакер, у которого нет информации об алгоритме, не будет даже знать, с чего *начать* расшифровку. Таким образом секретные алгоритмы дают некоторое преимущество по сравнению с теми, о которых известны подробности.

Несмотря на этот довод, большинство криптографических технологий, которые используются для защиты повседневной цифровой деятельности, опираются на общеизвестные алгоритмы. Вся информация о принципах их работы доступна в книгах и на веб-сайтах. Открыто публикуемым алгоритмам отдают предпочтение перед хранимыми в тайне, и тому есть две причины.

Первая состоит в том внимании, которое общеизвестные алгоритмы приковывают к себе. Чем больше людей обращаются к ним, тем крепче уверенность общества в их надежности. Представьте, что вы хотите купить очень безопасный замок для сарая, который возвели в своем саду для хранения золотых слитков (мечтать не вредно). Вы обращаетесь за советом к самому известному мастеру в своем городе. Он показывает вам линейку стандартных устройств – вариаций от традиционных, качественных замков, которые он продает всю свою жизнь. У него есть стенд с разрезанными моделями, чтобы подробно объяснить, как в этих замках работает каждый затвор и стержень. Но самым дорогим экземпляром в его магазине оказывается блестящий *WunderLock*, только-только появившийся в ассортименте. Вы спрашиваете, как он работает, и мастер признается, что он не имеет ни малейшего понятия, поскольку внутреннее устройство механизма WunderLock засекречено. Производитель его заверил, что замок надежный и стоит своей высокой цены, но сам мастер не ручается за его качество. Покупать или нет?

Предложение может показаться заманчивым. Если это и вправду отличный замок, он обеспечит вам дополнительную безопасность. Любой грабитель будет сбит с толку загадочным сверкающим предметом на двери сарая и, если повезет, любые попытки увести ваше золото закончатся неудачей. Таким образом покупка дорогого замка может окупиться, но в то же время вы рискуете. Вы вынуждены довериться производителю и его заявлениям о том, что замок действительно очень безопасный. У вас нет возможности опереться на опыт вашего местного (или, если уж на то пошло, любого другого) мастера. Большинство специалистов, которые всю жизнь исследуют устройство и безопасность замков, не смогут вам ничего подсказать о том, насколько в действительности хороша модель WunderLock.

Необходимо понимать, что эта проблема касается не только рекомендаций перед покупкой. Ваш новенький WunderLock может отлично служить год или два, пока однажды вы не обнаружите пустой сарай. Позже в новостях вы прочитаете, как находчивые воришки обнаружили, что настойчивое постукивание по WunderLock слесарным молотком отпирает его затвор. Об этом слабом месте стало бы известно раньше, если бы все слесари знали о внутреннем устройстве этого замка. Кто-то где-то как-то заметил бы этот дефект.

Не так давно (примерно полвека назад) криптографических алгоритмов было всего несколько, и в основном их использовали для военных задач и разведки. Мало кто в целом мире имел хоть какое-то представление об их устройстве и принципах работы. Алгоритмы разрабатывались под грифом строжайшей секретности, и, скорее всего, каждый специалист в этой области так или иначе имел отношение к разработке. Более того, эти специалисты пользовались полным доверием очень узкого круга избранных людей, прямо зависящих от этих алгоритмов.

И все это имело очень опосредованное отношение к криптографии в ее нынешнем виде. Можно выделить два важных отличия. Во-первых, в наши дни существует активное глобальное сообщество исследователей и разработчиков с опытом создания криптографических алгоритмов. Все они попросту не могут быть вовлечены в разработку *секретного* алгоритма. Любой алгоритм, внутреннее устройство которого засекречено, немедленно привлекает к себе повышенный интерес этого сообщества и может вызвать

подозрения. Если его не решились выставить на всеобщее обозрение и позволить желающим его проанализировать, может быть, с ним что-то не так? Во-вторых, мы *все* используем устойчивые криптографические алгоритмы, и потому нам необходимо им доверять[63]. Криптографический эквивалент WunderLock в основе системы безопасности здорово повышает градус риска. Зачем, если нам доступны проверенные алгоритмы, пользующиеся всеобщим уважением[64]?

Вторая причина, конечно, более основательна. В наши дни держать алгоритмы в тайне почти невозможно. Пятьдесят лет назад криптографические алгоритмы поставлялись в больших металлических ящиках с жестким ограничением доступа. Сегодня же криптография применяется в потребительских технологиях, и алгоритмы, реализованные в программном обеспечении, почти невозможно скрыть. Даже если они созданы чисто аппаратными, держать в тайне принципы их работы очень сложно, учитывая, сколько людей имеет доступ к начиненным ими устройствам. Специалисты могут проанализировать технологию и ее поведение, чтобы разобраться в работе алгоритма – этот процесс называется *обратным проектированием* (англ. reverse engineering[65]).

Любой, кто занимается внедрением секретных криптографических алгоритмов, должен исходить из того, что однажды (возможно, раньше, чем хотелось бы) они станут публичными. Об этом говорит не только свежий опыт. В конце девятнадцатого века, задолго до применения криптографии для компьютерных сетей, уважаемый датский криптограф Огюст Керкгоффс сформулировал шесть принципов проектирования криптографических алгоритмов[66]. В те времена алгоритмы (или системы, как называл их Керкгоффс) применяли вручную к письменным текстам. Керкгоффс был мудрым человеком. Вот один из этих принципов: *система не должна требовать секретности, и ее попадание в руки врага не должно вызывать проблем*.

Повесть о двух алгоритмах

Я убежден, что в сфере криптографии хранение рецептов в тайне не только вряд ли полезно, но и далеко не всегда возможно. В первую очередь это касается популярных рецептов, рассчитанных на широкое использование.

Давайте обсудим.

Рассмотрим два совершенно разных, но одинаково популярных во всем мире секретных рецепта. Производители Coca-Cola утверждают, что рецепт их напитка является одной из самых надежно охраняемых тайн в мире, и для его защиты предусмотрена тщательно продуманная процедура. Наличие секретной формулы для Coca-Cola чем-то похоже на попытку защитить мобильный телефон за счет использования секретного криптографического алгоритма. Сложно найти человека, который бы ни разу не пробовал Coca-Cola и не пользовался сотовой связью. Хранение в тайне алгоритмов, на которых основано то и другое, – крайне непростая задача.

Когда-то мобильные телефоны и правда были защищены секретными алгоритмами: архитекторы первых сотовых сетей считали, что это предоставляло дополнительную безопасность. Однако со временем эти алгоритмы были воссозданы и оказались не настолько безопасными, как было принято считать. Сегодня сотовые операторы согласны с тем, что преимущества глобальной известности их криптографических алгоритмов существенно перевешивают любую сомнительную пользу от их засекречивания[67]. В сфере мобильной связи секретные рецепты вышли из моды.

Так как же компании Coca-Cola удается успешно хранить свой рецепт в тайне? Дело в том, что этот рецепт, строго говоря, *не совсем* секретный. Процесс (алгоритм) создания газированных напитков широко известен, равно как большинство ингредиентов Coca-Cola специалисты уже опознали или угадали. И в самом деле, несколько компаний сейчас производят напитки, настолько похожие по вкусу на Coca-Cola, что большинство людей не может их отличить. Тайной окутано только происхождение одного из ингредиентов в этой формуле, известного как *Merchandise 7X*[68]. В этом отношении секретность 7X подобна секретности криптографического ключа. Алгоритм общеизвестен, но, заменяя 7X другими ароматизаторами, можно изобрести целый спектр газированных напитков. Как и в случае

с мобильными телефонами, рецепт Coca-Cola уже никто не скрывает, а уникальность напитка зависит от сохранности ключевого ингредиента.

Алгоритмы важны, но ключи принципиальны

Понимание того, что алгоритмам и ключам в криптографии отводятся разные роли – одна из действительно важных вещей.

Алгоритмы – это машинное отделение криптографии, которое определяет и проводит необходимые вычисления. С точки зрения пользователя, они работают в фоне, и на них можно не обращать внимания. Даже опытные специалисты по кибербезопасности редко работают с алгоритмами напрямую; им обычно достаточно знать, каким алгоритмом защищена система, за которую они отвечают.

Ключи – это секретные данные, на которые опираются механизмы безопасности, предоставляемые криптографией. В этом смысле они входят в состав интерфейса между технологиями и пользователями. В отличие от алгоритмов, общих для всех и вся, ключи уникальны и принадлежат отдельным пользователям или устройствам, а значит, требуют особого внимания. Криптографические алгоритмы, которые мы используем, известны всем. Но если кто-то завладеет нашими личными криптографическими ключами, все наши защитные меры в киберпространстве обнулятся.

Если говорить об использовании криптографии для обеспечения безопасности в киберпространстве, алгоритмы важны, но ключевую роль играют ключи.

3. Хранение секретной информации

Чтобы получить представление о полном спектре защитных механизмов, которые криптография предоставляет нам в киберпространстве, понятие *безопасности* следует разделить на несколько основных направлений. Первое из них – возможность надежно хранить секретную информацию.

Конфиденциальность

Когда людям предлагают поговорить о «защите» информации, большинству сразу же приходит на ум *конфиденциальность* – возможность выбрать, кто получит доступ к нашим (конфиденциальным) данным.

Секреты есть у всех. Речь идет не только о крайне деликатной информации, раскрытие которой унизит вас. Любые сведения, которые касаются вас и которые вы бы не хотели увидеть опубликованными в газете, секретны. Это все, чем вы с радостью делитесь с одними людьми, но скрываете от других. Определенно, ваши банковские реквизиты, пароли и PIN-коды относятся к этой категории, как и ваши адрес, дата рождения и семейные фотоальбомы. Представьте, что к вам на улице подошел незнакомец и начал настойчиво выспрашивать имена ваших детей и что вы вчера ели на ужин. Каким бы был ваш ответ? Если бы вы отказались, эти сведения тоже можно было бы считать секретными. У всех нас есть то, чем мы не хотели бы делиться со всеми и каждым[69].

Конфиденциальную информацию часто ассоциируют с *личной*, существование которой в более широком смысле объясняется желанием и возможностью скрывать от других те или иные сведения. Как высказался Эрик Хьюз в своем *«Манифесте шифропанка»*: «Личное дело – это то, чем мы бы не хотели делиться со всем миром, а секрет – то, что мы хотим скрыть ото всех. Приватность – это способность выборочно раскрывать информацию о себе»[70]. Механизмы безопасности, направленные на обеспечение

конфиденциальности, можно использовать для сохранения приватности, но приватность как таковая не ограничивается хранением секретов.

Конфиденциальность очень важна в материальном мире. Мы обеспечиваем конфиденциальность документов, запечатывая их в конверт, закрывая на ключ в картотеке или пользуясь услугами надежных курьеров. Мы понижаем голос и обсуждаем секреты за закрытыми дверями, чтобы ограничить круг тех, кто нас может услышать.

В киберпространстве хранение секретов становится необходимостью. Нужда в конфиденциальности возникает всякий раз, когда мы вводим личные данные на сайте, иначе хакеры, взломавшие этот сайт, смогут их заполучить. Конфиденциальность нужна во время разговора по телефону, чтобы его не могли прослушать случайные обладатели обычных радиоприемников. И уж тем более мы не хотим, чтобы при любой покупке в Интернете реквизиты банковской карты стали известны злоумышленникам. Проще говоря, когда мы хотим сохранить приватную информацию на компьютере, которому нельзя полностью доверять, нам нужна конфиденциальность. На самом деле это касается любого компьютерного устройства, включая ваши мобильник и автомобиль.

Иначе говоря, конфиденциальность необходима при передаче приватных данных по любой сети, к которой у нас нет полного доверия. И здесь тоже по большому счету речь идет обо всех сетях, включая Интернет и ваш домашний Wi-Fi[71].

Игра в прятки

Ребенок возвращается из школы с плохими отметками и не хочет, чтобы узнали родители. Этой информации срочно требуется механизм конфиденциальности! Ребенок кладет (то есть прячет) табель или дневник под матрас или в один из ящиков с одеждой.

Ключевой элемент успеха здесь состоит в том, чтобы тот, кто находится рядом с тайником, не видел очевидных признаков спрятанного объекта. Даже когда под матрасом спрятан дневник,

кровать выглядит как всегда. Выдвижной ящик по-прежнему в полном беспорядке после того, как под груду футболок положили табель.

Цифровая информация тоже может быть спрятана среди обычных, на первый взгляд, цифровых объектов. Примером этого может служить цифровое изображение. Оно состоит из сотен отдельных пикселей, которые человеческий глаз не способен различить ввиду их малого размера. У каждого пикселя есть определенный цвет, который, как и многие другие данные, представлен последовательностью битов. Некоторые из этих битов критически важны, другие используются лишь для тонкого регулирования итогового цвета. Изменение этих менее чувствительных битов пройдет незаметно для наблюдателя; следовательно, их можно с легкостью заменить другими битами с какой-то информацией, которую мы хотим скрыть. Сторонний наблюдатель увидит все то же изображение, но если знать, где искать, можно извлечь скрытую информацию.

Все мы в детстве играли в прятки и знаем, что прятаться – рисковое дело: тебя всегда могут найти. Табель с большой долей вероятности обнаружат во время уборки. А если кто-то заподозрит, что цифровое изображение может содержать скрытую информацию, анализ пикселей раскроет секрет.

Основное преимущество сокрытия по сравнению с механизмами конфиденциальности – то, что вы прячете не только информацию, но и сам факт ее существования. Пока родители провинившегося ребенка не встретят в школьном дворе знакомых и не начнут обсуждать отметки, они не узнают, что табель успеваемости уже выдали. Люди, рассматривающие цифровое изображение, даже не догадываются, что оно содержит какой-то секрет.

Тем не менее сокрытие факта существования информации не так уж и часто оказывается преимуществом. Если ваш банк решит отправить вам конфиденциальный документ, напечатанный на бумаге, вы, наверное, согласитесь с тем, что это лучше сделать традиционной почтой, запечатав документ в конверт; вам вряд ли захочется забирать документ в каком-то условленном секретном месте. Конечно, почтальон будет знать, что вы получили письмо от банка, но в конечном счете это не так уж важно. Важнее то, что он не может заглянуть в конверт. Точно так же, когда вы звоните кому-то по мобильному, вы не думаете о том, чтобы скрыть факт звонка,

конфиденциальным является сам разговор[72]. Или когда вы покупаете что-то в Интернете, конфиденциальным, как правило, остается не факт покупки, а детали транзакции.

Во всех этих примерах сокрытие информации оказывается не только лишним, но и нереалистичным. Как бы вы ее скрыли? Когда вы звоните кому-то, вы намерены отправить только данные, кодирующие ваш голос, а не какой-то дополнительный объект, в котором можно спрятать информацию о звонке. Любой цифровой объект, в котором можно было бы что-то скрыть, намного больше данных с конфиденциальным разговором, и это само по себе делает «игру в прятки» чрезвычайно неэффективной.

В целом сокрытие информации – не самый надежный способ обеспечения конфиденциальности. Раздел науки, изучающий механизмы сокрытия информации, называется *стеганография* (что в переводе с греческого буквально означает «тайнопись»[73]), и у нее есть определенные узкие сферы применения. С ее помощью преступник может скрыть инкриминирующие материалы на своем компьютере так, что никто даже не догадается об их существовании[74]. Стеганография применяется в сфере защиты цифровых прав, когда цифровой контент помечается особым образом без заметного ухудшения качества. Стеганография может пригодиться, если нужно укрыть какую-то информацию от правительства или руководства, объявившего использование механизмов конфиденциальности незаконным. Авторитарному режиму сложно обвинить человека в хранении секретов, если их существование нельзя доказать[75].

И все же полезнее прочих те механизмы обеспечения конфиденциальности, которые сохраняют информацию секретной, не скрывая факта ее существования. Их-то и можно реализовать с помощью криптографии.

Стеганография и криптография – разные вещи. Можно сказать, что стеганография эффективна в качестве механизма конфиденциальности только в том случае, когда сама скрытая информация уже зашифрована. Обычный человек использует стеганографию либо редко, либо вообще никогда, в то время как криптография стала неотъемлемой частью нашей повседневной жизни.

Взлом кодов

Допустим, у нас есть какая-то конфиденциальная информация, которую мы хотим отправить кому-то в киберпространстве. Нам не нужно скрывать тот факт, что она существует; мы просто хотим ограничить к ней доступ. Поскольку за процессом отправки может наблюдать кто угодно, эту информацию нужно как-то замаскировать. Иными словами, ее нужно отправить в измененном виде.

Как замаскировать информацию? Нам нужно привести ее к такому виду, чтобы она казалась бессмысленной любому постороннему наблюдателю. Следовательно, нам нужен алгоритм.

Давайте рассмотрим очень простой пример такого алгоритма. Допустим, информация, которую мы хотим защитить, состоит из букв, скажем, TOPSECRET. Это *обычный* (или исходный) *текст* – информация до того, как ее замаскируют. Чтобы проиллюстрировать этот процесс, я воспользуюсь *шифром Атбаш*[76] – изменением порядка следования букв алфавита на противоположный. Иными словами, каждая буква исходного текста заменяется буквой в той же позиции, но взятой из алфавита, записанного в обратном порядке: вместо A подставляется Z, вместо B – Y, вместо C–X и т. д. Полный алгоритм представлен в следующей таблице.

Обычный текст A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Зашифрованный текст Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Алгоритм шифрования Атбаш заменяет каждую букву в верхнем ряду этой таблицы буквой из нижнего ряда. Таким образом исходный текст TOPSECRET превращается в GLKHVXIVG. Эту вторую последовательность букв, которая может выглядеть бессмысленной, называют *зашифрованным текстом* или *шифротекстом*.

Шифротекст – это то, что мы отправляем предполагаемому получателю секретного сообщения. Любой, кто наблюдает со стороны, видит лишь GLKHVXIVG. Но получатель знает, что мы преобразовали простой текст в зашифрованный с помощью шифра Атбаш, поэтому

для восстановления оригинала он использует обратный алгоритм: заменяет каждую букву в нижнем ряду соответствующей буквой верхнего ряда. Таким образом получатель успешно избавляется от маскировки и превращает GLKHVXIVG обратно в TOPSECRET.

Насколько эффективен шифр Атбаш в качестве механизма конфиденциальности? Вообще-то он считается очень слабым по многим причинам, самая важная из которых связана с моим предыдущим наблюдением: нельзя полагаться на секретность самого алгоритма. Как утверждал Огюст Керкгоффс (и я с ним согласен), мы всегда должны исходить из того, что используемый нами алгоритм известен всем, даже если в реальности это не так. В примере применяется шифр Атбаш, поэтому следует предполагать, что о замене Z на A, Y на B и т. д. знают все. Следовательно, ни для кого не секрет, что шифротекст GLKHVXIVG соответствует обычному тексту TOPSECRET. Вот вам и конфиденциальность!

Проблема шифра Атбаш проста: любому, кто знает, что мы его используем, известно, как преобразовать зашифрованный текст обратно в обычный, поскольку для этого предусмотрен только один способ. Шифр Атбаш не может обеспечить конфиденциальность, поскольку совершенно лишен вариативности. Говоря иначе, его проблема в том, что это алгоритм без ключа.

Алгоритмы, шифрующие информацию без использования ключа, часто называют *кодами*. Обычно цель кода состоит в том, чтобы преобразовать информацию каким-то образом, но не для секретности. Наверное, самым известным кодом можно назвать азбуку Морзе, которая заменяет буквы короткими последовательностями точек и тире[77]. Она была разработана для передачи информации по телеграфу. Последовательности точек и тире позволяют превращать алфавитно-цифровые символы в короткие и длинные электромагнитные сигналы. Эта технология не имеет ничего общего с конфиденциальностью. Действительно, если бы международный сигнал бедствия «точка точка точка тире тире тире точка точка точка», переданный тонущим кораблем, не смогли расшифровать на проплывающем поблизости судне, это было бы катастрофой. Это шифротекст, который должен уметь расшифровать кто угодно.

Но иногда коды дают обманчивое ощущение конфиденциальности. Время от времени вам могут предлагать «взломать код» (я уже сбился

со счета, сколько раз мне говорили, что это моя работа как криптографа). На протяжении столетий египетские иероглифы представляли собой аналогичную проблему для исследователей Древнего Египта. Их значения удалось восстановить только в начале девятнадцатого века[78]. Однако иероглифическое письмо никогда не предназначалось для обеспечения конфиденциальности. С исчезновением древнеегипетской культуры люди просто забыли подробности алгоритма, который кодировал понятия в иероглифы. Повторного открытия этого алгоритма оказалось достаточно, чтобы наполнить иероглифы смыслом. Древние египтяне точно не стали бы рассматривать это как нарушение их безопасности.

Еще один известный код упоминается в романе Дэна Брауна *Код да Винчи*, посвященном секретам, загадкам и интригам[79]. Одна из главных героинь этого романа, криптограф Софи Неве, якобы училась в Королевском колледже Холлоуэй при Лондонском университете, где я в настоящий момент работаю. Во времена, когда эта книга лидировала в списках бестселлеров, многие новостные издания обращались ко мне с вопросами о криптографии, которую описывал Дэн Браун.

Тем не менее превосходное знание криптографии совершенно не пригодилось Софи Неве, поскольку в *Коде да Винчи* нет ничего криптографического. В раскрытии тайн и головоломок, которыми наполнена книга, Софи в основном помогает нестандартное мышление. Ближе всего к настоящей криптографии она оказывается в момент осознания, что одна из головоломок содержит текст, преобразованный шифром Атбаш. Поскольку этот шифр, как вам уже известно, не обеспечивает конфиденциальности, Софи почти моментально «вскрывает» секретное сообщение.

Итак, коды – это алгоритмы, с помощью которых можно маскировать информацию, но делается это обычно не в целях конфиденциальности. Если вы ищете механизм безопасности, который обеспечивает конфиденциальность, вам нужен алгоритм с ключом.

Делаем Атбаш конфиденциальным

Давайте «исправим» шифр Атбаш. Чтобы превратить его в нечто более полезное, буквы в исходном тексте должны кодироваться по-разному. В шифре Атбаш *единственный* способ кодирования переворачивает алфавит задом наперед. Но можно сделать так, чтобы это был лишь один из *многих* способов кодирования, а в идеале таких способов должно быть *неограниченное* количество. В результате получится так называемый *шифр простой замены*.

Шифр простой замены тоже проще всего представить в виде таблицы, только во втором ряду вместо обратного алфавита будет случайная последовательность букв без повторений. Как и Атбаш, этот алгоритм заменяет каждую исходную букву в первом ряду зашифрованной буквой снизу. Например, если шифр простой замены выглядит так:

Обычный текст A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Зашифрованный текст D I Q M T B Z S Y K V O F E R J A U W P X H L C N G

то строка TOPSECRET превращается в PRJWTQUTP. А если он имеет следующий вид:

Обычный текст A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Зашифрованный текст N R A W K I L F O C T E Y P V J S D B X H M Z U Q G

текст TOPSECRET будет закодирован в XVJBKADKX.

Можно ли считать это прогрессом? В шифре Атбаш алгоритм кодирования подставляет Z вместо A, Y вместо B и т. д. Конфиденциальность здесь невозможна, потому что алгоритм известен всем, и каждый знает, что буква A заменяется буквой Z и т. д. В шифре простой замены, представленном выше, алгоритм кодирования меняет A на N, B на R, C на A и т. д. Чем же это отличается от шифра Атбаш, учитывая, что алгоритм общеизвестный?

Разница на самом деле огромна! Ключевой ее аспект состоит в том, что алгоритм кодирования в шифре простой замены из нашего последнего примера не звучит как «заменить A на N, B на R, C на A и т. д.». Вместо этого его можно сформулировать так: заменить букву в верхнем ряду таблицы соответствующей буквой из нижнего ряда». Алгоритм знают все, но невозможно сказать, какая *именно* таблица была использована в конкретном случае. Эта информация отделяет тех, кому предназначено сообщение, от всех остальных. Конкретная таблица становится *ключом*.

Давайте посмотрим, как это работает. Представьте, что вы отправляете своему другу конфиденциальное сообщение с помощью шифра простой замены.

Сначала вам нужно договориться о секретном ключе, иными словами – условиться о случайной последовательности букв. Предположим, вам это каким-то образом удалось. Например, вы могли выбрать тот же ключ, который показан в нашем последнем примере – последовательность N, R, A, …, U, Q, G. Если вы хотите послать текст TIMEFORCAKE, вам нужно свериться с таблицей и заменить буквы в верхнем ряду соответствующими буквами из нижнего ряда: получится XOYKIVDANTK. Вы отправляете эту строку своему другу, и он, используя ту же таблицу, восстанавливает исходное TIMEFORCAKE.

Теперь посмотрим глазами злоумышленника, который хочет узнать содержание ваших секретных сообщений. Предположим, что ему известен алгоритм, то есть он знает, что вы используете шифр простой замены, и может видеть шифротекст, который вы отправляете. Если бы вы использовали Атбаш, злоумышленник мог бы легко восстановить исходный текст. Но он имеет дело с шифром простой замены и знает лишь то, что буквы исходного текста перемешиваются в соответствии с неизвестной ему последовательностью. Буква X в зашифрованном тексте, равно как O и Y, могла заменить любую другую букву.

Насколько безнадежна ситуация, в которой оказался злоумышленник? Что ж, у него всегда есть крайний вариант: он может попытаться подобрать неизвестный ему ключ. Поскольку ключ был сгенерирован произвольным образом, злоумышленник должен угадать случайную последовательность букв в алфавите, надеясь, что ему повезет. Чтобы вычислить вероятность успеха, необходимо

определить, сколько всего возможных комбинаций у последовательности из 26 букв.

Сделать это довольно легко. Первая буква может быть любой из 26, поэтому вариантов 26. В качестве второй буквы можно выбрать любую, кроме первой, поэтому остается 25 вариантов. Следовательно, существует 26 × 25 = 650 возможных комбинаций первых двух букв. Третья буква может быть любой, кроме тех двух, которые мы уже выбрали, поэтому остается 24 варианта. Таким образом для первых трех букв существует 26 × 25 × 24 = 15 600 комбинаций. И так далее.

В итоге получается, что число возможных последовательностей из 26 букв равно 26 × 25 × 24 × 23 × 22 × 21 × 20 × 19 × 18 × 17 × 16 × 15 × 14 × 13 × 12 × 11 × 10 × 9 × 8 × 7 × 6 × 5 × 4 × 3 × 2 × 1 = 403 291 461 126 605 635 584 000 000. Насколько большое это число? Чтобы не вводить все это в калькулятор, наберите «26» и нажмите кнопку с символом «!» (*факториал*). Если ваш калькулятор не очень мощный, эта операция может свести его с ума, и вместо результата он вернет сообщение об ошибке: ответ слишком большой. Более продвинутый калькулятор сообщит о том, что факториал 26 – это нечто невообразимое. Чего он вам не скажет, так это то, что данный ответ примерно в 40 000 раз превышает количество звезд во вселенной. Проще говоря, угадывание того, какой из возможных ключей выбрали вы с вашим другом – затея совершенно безнадежная, и злоумышленнику не стоит тратить на нее свое время.

Шифр Атбаш – это лишь один из 26! возможных вариантов шифра простой замены. Если ключ выбран случайным образом, вероятность получения шифра Атбаш или любой из двух других таблиц, описанных ранее, крайне низка. И каждый из этих ключей даже менее вероятен, чем выбор одной конкретной звезды, если бы звезд во вселенной было в 40 000 раз больше. Даже если в результате невероятного стечения обстоятельств вам выпадет ключ, соответствующий шифру Атбаш, это будет настолько ошеломляющим совпадением, что вряд ли злоумышленник о нем догадается.

С этой точки зрения шифр простой замены обеспечивает конфиденциальность. Но прежде чем вы приметесь шифровать с его помощью секретную информацию на своем компьютере, примите во внимание следующее: этот шифр действительно имеет 26! возможных ключей, но степень конфиденциальности, которую он предоставляет,

серьезно ограничена. Дело в том, что для получения исходного текста из зашифрованного вовсе не обязательно угадывать ключ. Существует куда более простой способ. Пока, впрочем, вам достаточно знать, что, в отличие от стеганографии и таких кодов, как шифр Атбаш, шифр простой замены является примером настоящего (хоть и несовершенного) криптографического механизма безопасности для обеспечения конфиденциальности.

Шифрование

Процесс обеспечения конфиденциальности с помощью криптографического механизма безопасности называется *шифрованием*. Любой метод шифрования состоит из *алгоритма*, который описывает основную процедуру кодирования обычного текста, и ключа, с помощью которого эта процедура варьируется. Алгоритм шифрования принимает на вход обычный текст и ключ, определяя процесс, который в итоге выдает зашифрованный результат. В случае с шифром простой замены роль алгоритма шифрования играет процесс замены букв в верхнем ряду таблицы буквами из нижнего ряда, а роль ключа – случайная последовательность, составляющая второй ряд.

Процесс, обратный шифрованию, называется *расшифровкой*. В ходе расшифровки закодированный текст и ключ передаются алгоритму, который возвращает исходный текст. Алгоритм расшифровки отменяет результат работы алгоритма шифрования. В случае с шифром простой замены он подставляет букву в верхнем ряду таблицы вместо буквы из нижнего ряда. Эти два алгоритма связаны между собой настолько тесно, что их обычно называют просто алгоритмом шифрования, поскольку расшифровка и так подразумевается.

Шифрование – это чрезвычайно важный механизм безопасности, и тому немало причин. Например, это древнейшая часть криптографии. Еще Юлий Цезарь, Мария Стюарт и Наполеон использовали криптографию для обеспечения конфиденциальности средствами шифрования. В двух мировых войнах двадцатого века, как и впоследствии во время холодной войны, на криптографии были основаны системы секретной связи.

Шифрование широко используется и в наши дни. Если вы сегодня звонили по мобильному телефону, сняли деньги в банкомате, подключились к Wi-Fi, купили что-нибудь в Интернете, задействовали VPN для доступа к офисному компьютеру из дома, смотрели платный телеканал или отправили сообщение в WhatsApp, это означает, что ваш день не прошел без шифрования.

Шифрование, наверное, можно назвать самым захватывающим применением криптографии, однако не следует забывать, что оно способно обеспечить лишь конфиденциальность. На сегодня оно редко используется самостоятельно, без криптографических механизмов, предоставляющих другие аспекты безопасности. Например, шифрование звонка в сотовой сети начинается только после того, как оператор применил криптографию для идентификации SIM-карты в телефоне. Шифрование банковской транзакции выполняется только в сочетании с другими криптографическими механизмами, которые следят за тем, чтобы никто не мог модифицировать сообщения во время их передачи.

Чтобы понять, почему шифрование обычного текстового сообщения не гарантирует, что полученный результат совпадет с текстом, который намеревался защитить отправитель, рассмотрим еще раз шифр простой замены. В одном из наших предыдущих примеров исходный текст TOPSECRET был зашифрован в XVJBKADKX. Этот процесс не позволяет злоумышленнику, получившему доступ к строке XVJBKADKX, узнать ее первоначальное значение.

Тем не менее ничто не мешает ему модифицировать шифротекст до того, как тот окажется у получателя. Злоумышленник мог бы, к примеру, поменять одну букву. Если он подставит X вместо J, расшифрованное сообщение будет выглядеть как POPSECRET. Опечатка ли это? Получателю остается только гадать (возможно, POPSECRET – это таинственный ингредиент в рецепте Coca-Cola!). Несмотря на то что злоумышленнику неизвестны конкретные последствия внесенного им изменения, получатель не может быть уверен в том, что расшифрованный текст корректен[80].

Традиционное шифрование

Если ненадолго вернуться к механизмам безопасности в материальном мире, можно назвать шифрование в некотором смысле цифровым эквивалентом хранения записки с текстом в закрытом ящике. Алгоритм шифрования (и расшифровки) – это цифровой аналог самого замкового механизма, а криптографический ключ можно сравнить с физическим.

Следует отметить, что физические замки бывают разных видов и конструкций. Чаще всего встречаются замки, для открытия и закрытия которых используется один и тот же ключ. Точно так же в стандартном (традиционном) шифровании ключ используется как для превращения исходного текста в зашифрованный, так и наоборот. Именно так работает шифр простой замены: ключ, необходимый и для шифрования, и для дешифровки, представляет собой случайную последовательность букв в нижнем ряду таблицы. Алгоритм, в котором для шифрования и дешифровки используется один и тот же ключ, называется *симметричным*.

Симметричное шифрование может показаться естественным. Интуиция нам подсказывает, что использование ключа любым другим образом бессмысленно. Как вообще возможно шифровать текст одним ключом, а расшифровывать другим? Однако напомню, что не все физические замки симметричны. В частности, тумблерно-штифтовые модели (которые обычно ассоциируют с компанией Yale) и многие навесные замки обычно запираются вообще без ключа. Ключ необходим только для их отпирания. Интересно, что у тумблерно-штифтовых и навесных замков есть криптографические эквиваленты. Механизмы, в которых для шифрования и расшифровки используются разные ключи, называются *асимметричными*.

Вплоть до 1970-х годов все механизмы шифрования были симметричными. Что общего у Юлия Цезаря, Марии Стюарт и Наполеона? Все они использовали симметричное шифрование. Даже Алан Тьюринг, один из тех гениев, кого в первую очередь ассоциируют с важной ролью криптографии во Второй мировой войне, мог бы посчитать идею асимметричного шифрования причудливой и нереалистичной[81].

В наши дни симметричное шифрование по-прежнему обладает наибольшей популярностью. Оно применяется для кодирования всех данных на вашем ноутбуке и при использовании Bluetooth. Оно

присутствует во всех повседневных примерах, рассмотренных ранее: Wi-Fi, мобильных телефонах, банковском деле, интернет-торговле и т. д. На самом деле для обеспечения конфиденциальности любых данных, будь то документы, электронные таблицы, веб-формы, электронные письма, голосовой трафик и т. п., неизменно используется симметричное шифрование. Большинство процессов шифрования симметричны. Этот подход так и оставался бы безальтернативным, если бы не одна небольшая проблема, о которой речь пойдет чуть ниже.

Алгоритмы симметричного шифрования эволюционируют по мере расширения наших знаний о том, как их лучше создавать (и взламывать). Прогресс в этой области был далеко непостепенным: и эта наука двигалась вперед резкими скачками.

Алгоритм шифрования, известный как *шифр Виженера*, был изобретен в середине шестнадцатого века, но применялся еще во время Гражданской войны в США. В конечном счете он оказался неустойчивым к методикам статистического анализа, разработанным во второй половине девятнадцатого века[82].

В электромеханических *машинах Энигма* были реализованы симметричные алгоритмы шифрования, основанные на электрических контактах, соединенных с последовательностью роторов. Они использовались почти всю первую половину двадцатого века, хотя пик их известности пришелся на Вторую мировую войну[83]. Эффективность использования машин Энигма в качестве механизмов симметричного шифрования свела на нет революция в области телекоммуникаций, последовавшая за изобретением цифровых компьютеров.

До недавнего времени симметричной криптографией пользовались в основном те, кому нужно было хранить самые серьезные секреты – правительственные и военные организации. Но с появлением в начале 1970-х годов коммерческих вычислительных устройств все изменилось. Потребность частных компаний в симметричном шифровании стала очевидной, особенно в финансовом секторе. В то время, и в какой-то степени до сих пор, предпочтение отдавалось секретным алгоритмам, поэтому для коммерческой криптографии нужен был новый, открытый вид симметричного шифрования, которым могли бы пользоваться все.

В 1977 году правительство США опубликовало симметричный алгоритм шифрования под названием *Data Encryption Standard* (стандарт шифрования данных), более известный пользователям как *DES*[84]. Это был воистину поворотный момент в истории криптографии, ознаменовавший ее превращение из *совершенно секретного* занятия в предмет всеобщего обозрения. *Стандарт* – то, что было проанализировано специалистами и одобрено для широкого использования. Создание стандарта шифрования было беспрецедентным и, естественно, способствовало применению DES в коммерческих организациях США, а впоследствии и многих других стран. Это был симметричный алгоритм шифрования, с которым могли взаимодействовать рядовые граждане в повседневной жизни (иногда сами того не осознавая).

На протяжении последних двух десятилетий двадцатого века почти все, кто обеспечивал конфиденциальность своих данных с помощью симметричной криптографии, использовали DES. Исключение составляли задачи, в которых требовалось особо быстрое шифрование трафика в режиме реального времени, как в случае с голосовыми данными. В таких областях часто применяются так называемые *потоковые* алгоритмы шифрования, которые кодируют каждый бит исходной информации мгновенно и по отдельности. Потоковые шифры тоже относятся к симметричным, но оптимизированы для высокой скорости и эффективности. В сравнении с ними DES представляют класс симметричных алгоритмов шифрования более общего характера – *блочные шифры*: они обрабатывают данные более крупными кусками (*блоками*).

К концу двадцатого века DES перестал считаться эффективным симметричным алгоритмом шифрования в основном потому, что вычислительные возможности постоянно росли и в какой-то момент достигли уровня, на котором DES больше не мог обеспечить достаточную безопасность. Тем не менее эта технология успела приобрести немалый авторитет, была встроена во множество систем, и полностью избавиться от нее до сих пор не вышло. За последние несколько дней вы с высокой вероятностью использовали, пусть и опосредованно, какую-то разновидность DES для шифрования каких-то данных, особенно если оплачивали что-то банковской картой.

Сделано в Бельгии

В современном симметричном шифровании применяется целый ряд разных алгоритмов. Банковские сети по-прежнему сильно зависят от DES, но ввиду того, что однократное применение DES давно уже не считается достаточно безопасным, данные обычно шифруются три раза с помощью расширенной версии этого алгоритма – *Triple DES*[85]. Однако в приложениях, требующих симметричного шифрования, все чаще используется блочный шифр *AES* (Advanced Encryption Standard – улучшенный стандарт шифрования)[86].

AES – еще один важный этап в истории криптографии. В середине 1990-х годов стала очевидной потребность в новом алгоритме симметричного шифрования, который можно было бы рекомендовать к использованию в постоянно растущем круге областей, где необходима конфиденциальность.

Между 1970 (когда был изобретен DES) и 1990-ми годами в мире криптографии произошло много важных изменений. Одно из них было связано с развитием Интернета и следствием этого – взрывным ростом деловой и повседневной активности в киберпространстве. Технологий, подключенных к глобальной сети, конечно, тоже стало больше, они стали разнообразнее и сложнее. Когда разрабатывался стандарт DES, симметричное шифрование в основном предназначалось для отдельных компьютеров наподобие банковских станций, поэтому архитектура DES была рассчитана на аппаратную реализацию. Но к 1990-м годам появился спрос на симметричное шифрование, эффективно реализованное на программном уровне, и заметно расширился спектр аппаратных платформ, которым нужно было симметричное шифрование. В 1970-х все компьютеры были похожи между собой. К 1990-м годам криптография применялась как на суперкомпьютерах, так и на крошечных устройствах вроде смарт-карт (пластиковые карты со встроенным чипом, похожие на кредитную карту).

Еще одно важное изменение затронуло общий уровень владения криптографией. В 1970-х большинство криптографов работало в правительственном и военном секторах, и знания концентрировались там же. За помощью в создании DES правительство США обратилось

к IBM – одной из немногих коммерческих компаний, которые в то время проявляли интерес к криптографии. К 1990-м годам активное сообщество криптографов сформировалось как в научных кругах, так и в частном секторе. Особенно это касалось телекоммуникационных компаний, чьи коммерческие империи опирались на эффективность криптографии.

Создание нового стандарта симметричного шифрования в духе двадцать первого века было поручено Национальному институту стандартов и технологий США (National Institute of Standards and Technology, NIST). Сотрудники NIST решили воспользоваться помощью сообщества криптографов за пределами правительства и организовали открытый конкурс по разработке нового алгоритма AES. Поскольку ожидалось, что новый симметричный алгоритм будет применяться по всему миру, к конкурсу были допущены не только американские компании, но и участники из других стран[87].

Это был кардинально новый подход к разработке криптографических алгоритмов. Неудивительно, что он привлек большинство ведущих специалистов в симметричном шифровании. Мой личный вклад в этот процесс состоял в попытке убедить моего коллегу по бельгийскому подразделению Винсента Рэймена переименовать алгоритм, который он разработал для конкурса вместе со своим другом Джоаном Дэеменом. Я не верил, что кто-то мог принять всерьез алгоритм под названием *Rijndael* (читается как «рейндал»), составленным из фамилий его создателей и вымышленной долины Ривенделл. Меня проигнорировали, в отличие от самого алгоритма. В 2001 году бельгийский алгоритм симметричного шифрования Rijndael стал стандартом AES.

Архитектура стандарта AES обладает элегантной простотой, что делает его реализации эффективными – и это во многом определило победу Rijndael. Возможно, вы думаете, что современные алгоритмы шифрования должны быть математически сложными и доступными для понимания только специалистам. Действительно, конкретные детали реализации неочевидны, и, чтобы в них разобраться, нужен определенный уровень знаний. Тем не менее основная идея, лежащая в основе AES, на удивление понятна и проста. Я попытаюсь приоткрыть завесу тайны, окружающую современное шифрование, и объяснить в самых общих чертах, как работает AES.

Как вы помните, алгоритм шифрования – это рецепт, состоящий из двух основных ингредиентов (исходного текста и ключа), которые смешиваются для получения зашифрованного результата. В AES это смешивание происходит следующим образом.

Форматирование исходного текста. Вначале обычный текст преобразуется в байты. Затем из первых 16 байт формируется матрица размером 4×4 байта[88]. Если после этого остается исходный текст, создается вторая матрица, потом третья и т. д. Если для формирования очередной матрицы размером 4×4 байта текста остается недостаточно, вместо недостающих байтов подставляется резервная информация, известная как *дополнение*. Теперь исходный текст готов к шифрованию.

Изменение всех байтов. Первый этап перемешивания исходного текста состоит в замене каждого байта матрицы новым байтом в соответствии с правилами алгоритма AES, поэтому все знают, как это делать. По окончании этого этапа получается квадратная матрица из 16 байтов.

Смещение строк. Этот второй этап перемешивания тоже крайне прост. Каждая строка матрицы сдвигается на определенное количество позиций; элементы, выступающие справа, вставляются слева.

Преобразование столбцов. Каждый столбец, состоящий из 4 байтов, преобразуется в соответствии со следующим правилом перемешивания в алгоритме. Все новые столбцы по-прежнему состоят из 4 байтов. В результате получается новая 16-байтная матрица.

Добавление ключа. На каждом из предыдущих этапов исходный текст перемешивается тем или иным образом, вроде того, как раздающий по-разному тасует карты. И только теперь в этот процесс добавляется ключ. Алгоритм AES описывает, как на основе ключа сформировать так называемый *раундовый ключ* – еще одну отдельную матрицу 4×4 байта. Добавив к нему матрицу исходного текста, мы получим еще одну квадратную матрицу из 16 байтов.

Повторение. Теперь, получив матрицу – смесь исходного текста и ключа, – мы снова включаем миксер, возвращаемся к этапу «изменение всех байтов», и процесс повторяется заново (*изменение всех байтов, смещение строк, преобразование столбцов, добавление ключа*), пока все не перемешается достаточно хорошо (в соответствии с AES). В самой простой версии (их существует три, с разной длиной

ключа) происходят десять повторений. Каждый полный цикл операций перемешивания называется *раундом* AES.

Вывод зашифрованного текста. Итоговая матрица размером 4×4 байта становится нашим зашифрованным текстом. Чтобы превратить зашифрованный текст обратно в исходный, весь процесс выполняется в обратном порядке.

Такова основная идея. Я опустил несколько тонкостей и не стал вдаваться в некоторые подробности. Моей целью было показать, что, по своей сути, алгоритм шифрования AES состоит из ряда относительно простых операций, совокупность которых позволяет получить зашифрованный текст, сохраняющий конфиденциальность исходной информации. Надеюсь, вы согласитесь с тем, что принцип работы AES прост и даже элегантен. Но не сомневайтесь, что изобрести такой алгоритм очень непросто[89].

Стандарт AES применяется для обеспечения конфиденциальности во многих современных технологиях. Например, вы, скорее всего, используете его каждый раз, когда устанавливаете защищенное соединение между своим браузером и сайтом (конечно, вы не выбираете AES сами, это делает браузер). Алгоритм AES настолько хорошо изучен и проверен, что по крайней мере в ближайшем будущем он, скорее всего, продолжит смещать строки и преобразовывать столбцы для защиты секретных данных.

Если вас когда-нибудь спросят, чем славится Бельгия, вы будете знать, что ответить. Картофель фри, пиво, шоколад и вымышленные гениальные сыщики – это замечательно, но Бельгия должна быть известна своей криптографией.

Вездесущий AES

Конечно, AES сегодня – далеко не единственный симметричный блочный шифр. С годами было предложено много альтернатив, включая финалистов того самого конкурса, которым лишь немного не хватило, чтобы стать стандартом AES. Существуют блочные шифры, названные в честь животных, скандинавских богов, бельгийских марок пива и даже чего-то малопонятного (вспомню лишь всеми любимый

шифр Hasty Pudding – пудинг на скорую руку). Поразительное множество блочных шифров названо в честь рыб[90]. Но лишь немногие из этих алгоритмов применяются в реальных разработках, и среди них AES, пожалуй, действительно важнейший.

Одна из причин, почему блочные шифры стали и остаются самыми распространенными механизмами для симметричного шифрования – гибкость их реализации. Как вы помните, блочный шифр кодирует блок (группу бит, чаще всего их 128) исходного текста в блок зашифрованного текста. Поскольку в 128 битах умещаются лишь 16 символов, мы обычно шифруем данные большего размера. Разделение текста на блоки с последующим шифрованием каждого в отдельности – не самая разумная мысль.

Основная идея состоит в том, что одинаковые блоки исходного текста в сочетании с конкретным ключом будут давать на выходе одинаковые зашифрованные блоки. Таким образом злоумышленник может выявить часто встречающийся исходный блок с помощью частотного анализа блоков шифротекста. Что еще хуже, если злоумышленнику каким-то образом удастся узнать, какой исходный текст соответствует конкретному зашифрованному блоку, он сможет сразу раскрыть все идентичные блоки.

Для борьбы с этой угрозой были разработаны более сложные методы шифрования, кодирующие больше одного блока за раз. Эти *режимы работы* блочного шифра разными способами связывают между собой шифрование отдельных блоков и наделяют шифры, в том числе (и прежде всего) AES, разными дополнительными свойствами, не ограничиваясь одной лишь конфиденциальностью. Например, некоторые режимы работы избавляют от необходимости дополнять последний блок, а другие позволяют обнаруживать изменения, внесенные в зашифрованный текст. Есть режимы, оптимизированные для определенных задач, скажем, для шифрования жестких дисков. Во многих задачах, для которых потоковый шифр подошел бы лучше, все равно используются блочные шифры в специальном режиме, фактически превращающем их в потоковые[91].

Итак, симметричное шифрование – самое распространенное средство обеспечения конфиденциальности, блочные шифры – наиболее широко применяемые его механизмы, а AES – несомненно,

самый популярный блочный шифр. Логично, что при таком раскладе наша безопасность в киберпространстве во многом зависит от AES.

Создает ли повсеместное распространение AES какие-то проблемы? В конце концов, самые здоровые экосистемы – биологически разнообразные, а зависимость от той или иной продовольственной культуры может привести к катастрофе. Не должно ли и в криптографии быть больше разнообразия?

В какой-то мере зависимость от AES рискованна, но этот риск оправдан. AES никогда не даст вам абсолютных гарантий безопасности, однако подобные стандартизированные криптографические алгоритмы исследуются намного активней, чем их аналоги. И поскольку никто за все прошедшее время не сообщил о проблемах, уверенность в AES растет.

Иногда нам выпадает случай продемонстрировать свой вкус, например, при выборе одежды для вечеринки или обстановки в комнату. Но, покупая что-то сугубо функциональное, вроде посудомоечной машины, лучше забыть о модных веяниях и отдать предпочтение надежной марке и модели. В этом отношении механизмы шифрования намного больше похожи на посудомоечную машину, чем на вечернее платье. Если в AES когда-нибудь обнаружится серьезный недостаток, его немедленное исправление будет в интересах всего мира. Используя менее популярный блочный шифр, вы, может быть, меньше подвержены этой конкретной угрозе; однако оборотная сторона такого выигрыша – повышенный риск того, что ваш шифр исследовался недостаточно тщательно и на самом деле не так уж надежен и безопасен.

Проблема распространения ключей

Симметричное шифрование – прекрасный инструмент, который мы постоянно используем. Однако у него есть очевидный недостаток: и для шифрования, и для расшифровки обязательно нужен секретный ключ. Один и тот же. Чтобы этот инструмент работал, все, кому нужен ключ, должны его каким-то образом получить.

Но каким образом происходит распространение ключей? Мы не можем просто рассылать их по мере необходимости обычными

средствами связи, поскольку ключи к секретной информации и сами – секретная информация. Злоумышленник может получить доступ к большинству коммуникационных каналов в киберпространстве, таких как Интернет. Что же обычно делают, когда нужно послать ключ? Естественно, его шифруют! Но для того, чтобы что-то зашифровать, нужен… ключ. Да, вам не померещилось. Чтобы передать кому-то ключ, вам нужен ключ. Своего рода криптоверсия проблемы курицы и яйца[92].

В материальном мире у нас редко возникают трудности с транспортировкой ключей туда, где они нужны. Когда мы закрываем какой-то замок, открывать его позже, вероятно, придется тоже нам, поэтому ключи отправляются в карман. Мы обычно не обмениваемся секретными сообщениями в закрытых ящиках и не беспокоимся о том, что кто-то посторонний завладеет ключом и сможет заглянуть внутрь. Иными словами, мы не сталкиваемся с серьезной *проблемой распространения ключей*, с которой имеют дело пользователи средств симметричного шифрования.

Распространение ключей симметричного шифрования, впрочем, тоже не всегда вызывает трудности. В тех редких случаях, когда нам нужно дать кому-то физический ключ, мы, как правило, делаем это лично: если вам захочется одолжить гостю ключ от дома, вы просто отдадите его при встрече. Если встретиться по какой-то причине невозможно, вы оставите ключ где-то поблизости (например, под цветочным горшком).

Точно так же физическая приближенность может использоваться для распространения ключей для симметричного шифрования. Неплохой пример – домашняя беспроводная сеть. Соединения со всеми устройствами в ней защищены с помощью симметричного шифрования. В качестве основы секретного ключа, с помощью которого шифруется трафик, выступает основной ключ для доступа к Wi-Fi – пароль. У владельца сети должна быть возможность сгенерировать этот главный ключ. Несмотря на то что владелец часто записывает свой пароль на клочке бумаги (как правило, чтобы не суметь отыскать потом), проще всего его найти на корпусе маршрутизатора, управляющего беспроводной сетью. Любое новое устройство, чтобы присоединиться к сети, должно использовать симметричное шифрование, а значит, снабжено этим паролем.

Главный ключ можно ввести в устройство вручную, можно и установить автоматически, если маршрутизатор физически рядом. Варианты одинаково действенны: никакое устройство не сможет подключиться к сети Wi-Fi, если находится действительно далеко от маршрутизатора (или владельца)[93].

В материальном мире нам бывает нужен новый ключ. За ним мы обычно обращаемся к доверенному лицу – человеку, с которым у нас как минимум есть деловые отношения. Например, ключ от нового дома нам, как правило, вручает агент по недвижимости (полностью ли мы ему доверяем – это уже другой вопрос). Точно так же ключи от новой машины нам выдает автосалон, которому мы доверяем достаточно, чтобы передать ему деньги в обмен на колеса. Многие практические способы применения симметричной криптографии, направленные на защиту секретных данных, возлагают распространение ключей на какую-то доверенную сторону. Симметричный ключ для кредитной карты мы получаем непосредственно от банка вместе с самой картой. Симметричный ключ для мобильного телефона мы получаем на SIM-карте непосредственно от оператора или посредников, которые продают контракты от его имени. Примечательно, что в этих двух примерах мы получаем ключи задолго до того, как в них возникнет необходимость.

Но иногда в киберпространстве нужно делать вещи, речь о которых вообще крайне редко заходит при использовании физических замков и ключей. Я говорю о предоставлении незнакомцам доступа к секретной информации.

Рассмотрим конкретный пример. Представьте, что вы решили приобрести виджет в интернет-магазине, с которым прежде не имели дела. Вы хотите, чтобы детали оплаты остались конфиденциальными, поэтому у вас возникает необходимость в криптографическом ключе. Магазин далеко, и вы не можете просто подъехать и забрать свой ключ лично. И деловых отношений, от которых мог остаться согласованный ключ (например, карта лояльности с ключом на чипе), у вас с этим магазином раньше не было. Ситуация усугубляется тем, что виджет вам нужен прямо *сейчас*, и вы не хотите ждать, когда ключ будет доставлен какими-то физическими (и дорогими) средствами.

Такой обмен секретной информацией с незнакомцем может на первый взгляд показаться нерешаемой задачей. Но ее, как и многие

другие с виду неприступные проблемы, можно решить с помощью криптографии. Однако для этого требуется кардинально другой тип шифрования.

4. Обмен секретной информацией с незнакомцами

В начале 1970-х годов существовал только один вид шифрования: симметричный. Но уже к концу десятилетия появилась альтернатива. Сложно сказать, насколько революционной была идея асимметричного шифрования: она с самого начала была направлена на решение проблемы распространения симметричных ключей и позволила двум людям, которые предварительно не согласовали ключ, сделать это на виду у злоумышленника.

Асимметричное шифрование может показаться волшебством. И это недалеко от истины. Оно способствовало развитию многих других потрясающих технологий, ставших возможными благодаря криптографии: цифровых подписей, электронных платежей в цифровой валюте и голосования через Интернет.

Огромная связка ключей

Чтобы по достоинству оценить возможности асимметричного шифрования, вернемся к предыдущему примеру, в котором вам неожиданно понадобился ключ для шифрования взаимодействия с незнакомым сайтом. Что вам потребовалось бы для решения этой задачи с использованием одной лишь симметричной криптографии?

Я уже отмечал, что ключ можно было бы доставить какими-то физическими средствами. Вы или работники магазина могли бы сгенерировать криптографический ключ и договориться о передаче его другой стороне – лично или, скажем, с помощью службы доставки. Это стоило бы вам денег и, что важнее, времени. В контексте интернет-покупок эта идея выглядит нелепо.

Ключами можно было бы обменяться еще до того, как зайти на сайт. Но поскольку у каждого сайта должен быть ключ не просто отдельный, но и уникальный, вам пришлось бы запастись ключами для всех онлайн-ресурсов, которые вы собираетесь когда-либо посетить.

Главная проблема этого подхода в его масштабности. В киберпространстве более 1,5 миллиарда сайтов[94]. Ради возможности когда-нибудь зайти на любой из них вам придется хранить более 1,5 миллиарда симметричных ключей. Учитывая, что доступ в Интернет есть примерно у половины населения планеты, каждый продавец, который хочет сделать свой товар доступным, должен хранить 3,5 миллиарда ключей.

Интересно, что проблема отнюдь не в емкости хранилищ. Если бы каждый из этих ключей был создан в формате AES длиной 128 бит, то для них всех продавцу пришлось бы выделить 45 гигабайт (карта памяти такого объема стоит меньше, чем обед на двоих в дешевом ресторане). Кошмарной идею делает необходимость управлять всеми этими ключами. Как вы будете их распространять? Как вы будете следить, к каким сайтам относятся какие ключи? Как справиться с тем, что каждую минуту каждого дня в году появляются все новые и новые сайты?

Есть еще один вариант: можно было бы создать глобальный центр обмена ключами, которому доверяли бы все пользователи Интернета. Каждый из нас мог бы заранее получить свой симметричный ключ, например, на смарт-карте, подобно тому, как банк выдает вам ключ в конверте с банковской картой. Если вам нужно сгенерировать новый ключ для безопасного взаимодействия с сайтом, вы тоже можете обратиться в глобальный центр, и результат будет отправлен вам зашифрованным при помощи ключа, который есть как у центра, так и у вас. Похожим образом тот же ключ отправлялся бы и сайту.

Все просто?

Ах если бы.

Первыми вступят в игру проблемы политического характера. Кому все пользователи Интернета могут доверить создание такого глобального центра ключей? Американцы не доверяют русским, те не доверяют британцам, которые, в свою очередь, с подозрением относятся к французам, которые не в восторге от руританцев и т. д. Возможно, эту обязанность можно было бы возложить на ООН, но даже если это сработает, встанет проблема централизованности такой конструкции: каждый раз, когда кто-то захочет с кем-то пообщаться, им обоим придется сначала обратиться в глобальный центр ключей. Это невероятно замедлило бы любые взаимодействия. К тому же, если

глобальный центр окажется временно недоступным или скомпрометированным, последствия будут катастрофическими.

Однако стоит отметить, что решение с центром ключей идеально подходит для отдельных организаций. Какая-то частная компания вполне может предоставить каждому работнику по ключу. Более того, у многих компаний есть собственные централизованные сети, что делает запрос ключей из центрального хранилища действенным решением. Правда, такие пользователи, связанные с центром ключей через работодателя, не будут в полной мере «незнакомцами»[95]. А в масштабах многочисленного и менее структурированного населения (читай – все или почти все пользователи Интернета) это просто не будет работать.

Итак, для обмена ключами с незнакомцами одного лишь симметричного шифрования, как правило, недостаточно.

Сумасшествие с навесными замками

Чтобы понять, как лучше обмениваться секретной информацией с незнакомцем, попробуем вдохновиться примером из реального мира. Возможно, это нелепая и немного надуманная история, но я надеюсь, что она будет достаточно наглядной.

Представьте, что вы получили имя и адрес незнакомца, живущего на другом конце города, и вам нужно написать ему конфиденциальное письмо. Звучит неправдоподобно, поэтому пусть незнакомцем будет юрист, с которым вы уже говорили по телефону, но не встречались, а передать вы хотите свое завещание.

Проще всего было бы запечатать письмо в конверт и бросить в почтовый ящик. Но какой бы замечательной ни была почта, всегда может найтись слишком любопытный работник, который откроет конверт с помощью пара и заглянет внутрь. Чтобы избежать этого, письмо можно было бы положить в чемодан, который закрывается на ключ, и отправить его курьером. Но где юрист возьмет ключ, чтобы открыть чемодан?

Как вы помните, физические замки бывают двух типов. Одни открываются и закрываются одним и тем же ключом, другие,

навесные, требуют ключ только для открытия, а закрыть их может кто угодно.

Рассмотрим другую версию той же истории: вы кладете письмо в чемодан и закрываете его навесным замком, ключ к которому есть только у вас. Курьер отвозит ваш чемодан юристу[96]. Он надежен, но по дороге может попытаться заглянуть внутрь, чтобы прочитать письмо – отсюда и необходимость в замке (криптографы назвали бы такого курьера «честным, но любопытным»).

Получив чемодан, юрист не может его открыть: у него все еще нет ключа к вашему навесному замку. Поэтому он вешает на чемодан еще один замок, ключ к которому есть только у него, возвращает чемодан курьеру и просит передать его вам. Этот чемодан никогда еще не был настолько защищенным: у него теперь есть два замка, и ни у кого нет ключей к обоим.

Приняв чемодан, вы открываете свой навесной замок, а другой оставляете, и снова просите курьера доставить его юристу. Раздраженный, но явно довольный тройной оплатой, курьер снова везет чемодан на другой конец города. И наконец на этот раз юрист открывает свой замок и извлекает письмо.

Сумасшедшая, но рабочая процедура. Что же на самом деле происходит? Чемодан катается туда и обратно, чтобы на нем в итоге остался замок, который может открыть юрист. Это вполне рабочее и довольно забавное, но все-таки переусложненное решение для безопасной доставки конфиденциального письма. Однако небольшая корректива могла бы сэкономить вам время и деньги, а также сократить выбросы углекислого газа (если курьер ездит не на велосипеде). Вы могли бы сначала позвонить юристу по телефону и попросить его прислать навесной замок. Получив его, вы могли бы повесить этот замок на чемодан, вручить тому же курьеру и отослать все вместе обратно юристу.

Эта идея с навесными замками по-прежнему кажется немного громоздкой, но это уже лучше, чем тройная доставка. Что важнее, именно на этой модели основано асимметричное шифрование.

Навесные замки в киберпространстве

Настоящий навесной замок приходится доставлять физическими средствами. Но что если бы вопреки всем законам физики он мог бы мгновенно телепортироваться туда, где он нужен? В этом случае мы бы получили эффективное решение проблемы обмена секретной информацией с незнакомцами в материальном мире.

К счастью, в киберпространстве телепортация почти возможна. На концептуальном уровне цифровой «навесной замок» можно передать со скоростью света (например, по электронной почте) и затем с его помощью «защелкнуть» цифровой эквивалент чемодана. Реализация этой идеи позволила бы нам обмениваться секретной информацией с незнакомцами, поскольку при подключении к сайту, который мы никогда прежде не посещали, было бы достаточно воспользоваться цифровым навесным замком. Именно это делает возможным асимметричное шифрование.

Навесной замок теоретически может закрыть любой, но открыть его может только тот, у кого есть ключ. Таким образом его цифровой аналог представляет собой вид шифрования, доступный кому угодно, тогда как возможность расшифровки остается только у заданного получателя. В связи с этим криптографический ключ должен быть известен всем, то есть не должен быть секретным. Такой ключ называют *открытым*, так как его можно сделать публично доступным. По этой причине асимметричное шифрование часто называют *шифрованием с открытым ключом*.

С другой стороны, заданный получатель должен быть единственным, кому под силу открыть цифровой навесной замок. Как и в симметричном шифровании, ключ, используемый для расшифровки, должен храниться в тайне. Его обычно называют *закрытым ключом*, поскольку он принадлежит только получателю, и его нельзя никому раскрывать (аналогично ключу для настоящего, физического навесного замка). В асимметричных шифрах для шифрования и расшифровки используются *разные* ключи. Тем не менее эти ключи должны быть как-то связаны между собой.

Давайте поразмыслим, что требуется для асимметричного шифрования. Зашифровать данные с помощью открытого ключа может любой, но расшифровать их может только тот, у кого есть закрытый ключ. Таким образом процесс шифрования доступен всем, но только закрытый ключ позволяет его обернуть вспять. Как это возможно?

Если подумать, то жизнь полна примеров того, что легко сделать, но сложно вернуть в первоначальный вид. Взять хотя бы приготовление ужина. Состряпать что-то вкусное с нуля легко, но извлечь исходные продукты из уже приготовленного блюда обычно невозможно, так как химические процессы необратимо изменили их и связали между собой.

Готовка – хорошая, но не идеальная аналогия для асимметричного шифрования, поскольку изначальные ингредиенты уже *невозможно* получить обратно. В асимметричном шифровании мы хотим сделать обратный процесс невозможным для всех, кроме *одного* человека – владельца закрытого ключа. Таким образом, расшифровка возможна, но только в особых обстоятельствах. В связи с этим нам придется смириться с небольшим компромиссом. Тем, кому неизвестен закрытый ключ, должно быть *крайне сложно* выполнить расшифровку[97].

Метод асимметричного шифрования должен состоять из действий, которые легко выполнить на компьютере, но очень сложно обратить. Превратить людей в интернет-рабов? Забрать их свободное время? Спровоцировать бессонницу? Все это действительно сложно исправить, но нам нужно что-то более точное. Мы должны выбрать *вычислительную задачу*, которая не составит труда для компьютеров, но ее результаты будут сложно обратимыми.

Мигающий курсор

Чтобы получить представление о разработке методов асимметричного шифрования, стоит поговорить о том, что компьютеру делать *сложно*.

Представьте, что вам нужно решить непростую вычислительную задачу. Не жалея денег, вы купили мощный компьютер, запрограммировали его и нажали клавишу **Enter**. Компьютер начал усердно работать. Прошло несколько часов, затем дней. По прошествии недель и месяцев он начал нагреваться. В итоге из его задней панели пошел дым. Что дальше? Купить компьютер побольше и помощнее?

Возможно! Но лучшее ли это решение? Компьютеры – чрезвычайно мощные устройства, способные на удивительные вещи, однако некоторые вычислительные задачи быстро выходят из-под контроля даже на самом производительном оборудовании. Если попросить компьютер выполнить такую задачу, он, может, и не задымит, но результат вы точно не получите.

Чтобы понять, почему это происходит, представьте себе задачу, вполне посильную для человека, но требующую некоторых усилий. Еженедельная уборка в доме подойдет. Сколько времени у вас на нее уходит, скажем, полдня (я живу с человеком, который назвал бы такую оценку оптимистичной)? Да, это работа, и она утомляет, но ее можно выполнить в приемлемые сроки. Допустим, у вас талант к уборке, и вы решили этим зарабатывать. Для начала вам придется прорекламировать свои услуги.

Самая очевидная маркетинговая стратегия – договориться с соседями. Женщина из соседнего дома просит вас прибрать ее дом, и вот у вас уже есть полдня оплачиваемой работы. Потом оказывается, что уборщик нужен семье дальше по улице, да и их соседям по обе стороны. Позвонив еще в несколько дверей, вы расширяете список клиентов до шести. Это уже постоянная работа. Можно было бы остановиться, но вы обнаруживаете, что спрос на услуги уборщиков в вашем районе довольно высок. Вы нанимаете работника, потом другого, и вскоре вам удается построить небольшой бизнес. Можно сказать, что ваше молодое предприятие имеет успех в мире коммерции, и важно, что вам удается полностью контролировать его уверенный рост.

Теперь давайте рассмотрим другую маркетинговую стратегию. В этом сценарии вы решили рекламировать свои услуги в социальных сетях. Допустим, у вас есть 100 друзей, и 10 из них откликнулись на ваше предложение. Это значит, что вы сразу получили работу на неделю вперед. Теперь представим, что в ходе своей рекламной кампании вы попросили друзей поделиться этим предложением со *всеми*, с кем они дружат. Предположим, что у каждого из них по 100 других друзей, с которыми вы не знакомы, и доля положительных откликов среди них та же (в этом примере мы много всего допускаем, поэтому не стоит зацикливаться на подробностях). Таким образом с вашим предложением ознакомилось целых 10 000 человек, и на вас

обрушилась тысяча заявок на уборку. Ого! Если вы не хотите терять этот шанс, вам срочно нужно нанять не меньше сотни уборщиков!

Неожиданно для себя вы начали превращаться из мелкого частного предпринимателя в важную по локальным меркам компанию. Если, упаси боже, каждый из этих 10 000 друзей ваших друзей покажет ваше объявление *своим* друзьям, круг ваших потенциальных клиентов расширится до миллиона, и вам придется готовиться к еще 100 000 заявок. В мгновение ока затея вышла из-под контроля. Всего за два дополнительных цикла этой вирусной рекламной кампании у вас окажется миллиард клиентов и перспектива убирать все – от иглу в Арктике до соломенных хижин в Калахари.

Суть этого примера в том, что некоторые задачи хорошо и просто масштабируются по мере увеличения чисел, а другие растут экспоненциально и неуправляемо. Это в равной степени касается как домашней уборки, так и вычислительных задач. С некоторыми вещами компьютеры справляются легко. Например, они умеют очень хорошо складывать. Вы можете вводить все большие и большие числа, и компьютер будет покорно возвращать вам их сумму, словно собака палку. В какой-то момент компьютер достигнет предела своих вычислительных возможностей и откажется выдавать ответ. Если вам все равно необходимо сложить эти гигантские числа, достаточно будет купить компьютер помощнее. Но некоторые вычислительные задачи работают совсем иначе: подобно нашему примеру с вирусной рекламой они быстро выходят за рамки возможностей *любого* компьютера. Даже если взять самое мощное оборудование в мире, в ответ удастся получить лишь мигающий курсор, который так и продолжит мигать, пока вы живы[98].

Именно сочетание этих разновидностей вычислительных задач необходимо для реализации асимметричного шифрования. Алгоритм шифрования должен быть относительно простой операцией, доступной любому компьютеру. Но компьютер, который попытается выполнить алгоритм расшифровки без ключа, будет лишь беспомощно мигать курсором точно как вы, если бы вам на завтра нужно было найти 100 миллионов уборщиков.

Простой множитель

Немногие по-настоящему понимают роль криптографии в защите компьютерных систем (вы как раз на пути к тому, чтобы стать исключением), но один факт, похоже, общеизвестен: безопасность компьютеров имеет какое-то отношение к *простым числам*[99]. В криптографии они используются повсеместно, однако именно их роль в алгоритмах асимметричного шифрования привлекла к ним больше всего внимания.

Простые числа – это целые числа больше 1 с одним общим элементарным арифметическим свойством: они должны делиться без остатка только на себя и 1. Самое малое из них – 2 (и это единственное четное простое число, поскольку все остальные четные числа делятся на 2 без остатка). Дальше идут 3, 5 и 7. А вот число 9 уже не простое, так как делится на 3. Следующие простые числа – 11 и 13, но не 15, которое делится на 3 и на 5. Эту цепочку можно продолжать до бесконечности, поскольку простых чисел бесконечно много.

В каком-то смысле простые числа – элементарные компоненты всех целых чисел, потому что любое целое число можно получить путем умножения нескольких простых. Например, $4 = 2 \times 2$, $15 = 3 \times 5$, $36 = 2 \times 2 \times 3 \times 3$. Собственно, любое целое число и есть результат перемножения одного уникального набора простых чисел. Например, $100 = 2 \times 2 \times 5 \times 5$. Никакой другой набор простых чисел, умноженных друг на друга, не даст 100. Таким образом простые числа 2,2,5,5, известные также как *простые множители* 100, составляют его уникальную «ДНК».

Эта прямая связь между числом и его простыми множителями лежит в основе самого известного асимметричного алгоритма шифрования, *RSA* – по именам его создателей Ривеста, Шамира и Адлемана (Rivest, Shamir и Adleman[100]). Отношения между числом и его простыми множителями формируют типы вычислительных задач, идеально подходящие для асимметричного шифрования: в одном направлении они выполняются относительно легко, а в противоположном оказываются непосильными даже для компьютера.

Простое направление состоит в умножении. Умножить два любых простых числа способен не только компьютер, но и вы сами, если не зевали на уроках математики. Проверьте, если хотите: попробуйте по порядку умножить следующие простые числа, желательно в уме

(используйте ручку и бумагу только в случае необходимости!): 3 × 11,5 × 13, 7 × 23, 11 × 31, 23 × 23, 31 × 41.

Как вам такое упражнение? С каждой парой чисел вам, вероятно, требовалось все больше времени, но вряд ли хоть раз вы провозились дольше, чем наливали бы чашку чая.

Позволь вы себе ручку и бумагу, вам, несомненно, удалось бы перемножить более впечатляющие простые числа. Ну-ка, сколько будет 23 189 на 50 021 (не ленитесь, ответ вам понадобится чуть ниже). Используя навыки, мало чем отличающиеся от тех, которые вы усвоили в школе (если вам не удалось справиться с последним упражнением, вы просто подзабыли изученное), компьютеры могут перемножать по-настоящему огромные целые числа. В этом смысле умножение является простой вычислительной задачей. Время вычисления растет по мере роста чисел, но получить результат по-прежнему несложно.

Обратная операция заключается в вычислении простых множителей заданного значения. Мы можем даже знать, что оно состоит из *двух* простых чисел, умноженных друг на друга. Вопрос в том, *что* это за числа. Эта задача не выглядит слишком устрашающей и непосильной, однако на компьютере она очень скоро выходит из-под контроля. Числа становятся все больше и больше, и в какой-то момент (неожиданно быстро) даже самые мощные суперкомпьютеры в мире, такие как китайский Sunway TaihuLight с почти 100 петафлопсами[101] вычислительной мощности, начинают растерянно мигать курсорами[102].

Чтобы получить представление о том, почему вычисление множителей так быстро усложняется, найти два простых множителя для каждого из следующих чисел: 21, 35, 51, 91, 187, 247, 361, 391. Обратите внимание на то, что по мере продвижения вам нужно все больше и больше времени (а ваша голова болит все сильнее).

Сдались, так и не дойдя до конца? А ведь это совсем маленькие числа в глобальных масштабах. Как насчет 83 803? Или, еще лучше, 1 159 936 969? Если у вас уцелел тот листок бумаги, на котором вы демонстрировали свои навыки умножения, вы можете обнаружить, что 1 159 936 969 = 23 189 × 50 021. Но смогли бы вы получить этот результат в уме? Сомнительно, если учесть, что самая очевидная тактика разложения числа на множители заключается в том, чтобы

поделить его сначала на наименьшее простое число (2), затем на следующее (3), затем на 5 и т. д. Вам пришлось бы перебрать 2586 простых чисел, пока вы добрались бы до нужного[103]!

Тем не менее в криптографических масштабах 23 189 и 50 021 – это очень мелкие простые числа. В настоящее время в RSA рекомендуется использовать как минимум 450-значные простые множители[104]. Несмотря на такую огромную длину, вы легко перемножите их на своем ноутбуке. Но если поручить суперкомпьютеру Sunway TaihuLight найти эти два простые множителя, в ответ он только замигает…

Цифровые навесные замки с разложением на множители

Безопасность алгоритма асимметричного шифрования RSA опирается на сложность вычисления простых множителей. Если не вдаваться в подробности, основная идея выглядит так.

Когда вам нужно создать цифровой навесной замок, вы сначала генерируете два огромных простых числа, порядка 450 цифр каждое. Эти числа нужно хранить в тайне, так как они, в сущности, составляют ваш секретный ключ (на самом деле ваш ключ – это не просто их сочетание, а то, что из них можно получить, но это уже детали), их должны знать только вы.

Теперь эти два простые числа нужно перемножить. Примерно 900-значный результат этой операции в сочетании с другим значением будет вашим открытым ключом. Вы можете разослать его всем друзьям, опубликовать на своем сайте, да хоть напечатать на визитке. Ваш открытый ключ может увидеть кто угодно. Сложность разложения числа на простые множители гарантирует, что ни у кого нет достаточно мощного компьютера, способного их определить, хотя оба они закодированы в открытом ключе.

Детальное понимание работы шифрования RSA требует знания некоторых аспектов математики университетского уровня, но мы можем это пропустить[105]. Важно то, что любой, кто хочет послать вам зашифрованное сообщение, должен сначала получить ваш открытый ключ (это делается легко, ведь его никто не прячет). Исходный текст

преобразуется в число (для этого предусмотрены стандартные методы), а сам же процесс шифрования состоит из последовательных операций умножения с участием исходного текста и вашего открытого ключа.

Шифрование возможно благодаря тому, что умножать числа компьютеры умеют не хуже, чем складывать. Получив зашифрованный текст, вы можете применить к нему операцию расшифровки. Она, конечно, тоже выполнима, так как состоит из последовательности умножений, но на этот раз с участием зашифрованного текста и вашего закрытого ключа. Любому, кто перехватит зашифрованный текст и захочет его прочитать, придется каким-то образом обернуть процесс шифрования вспять, не владея закрытым ключом. Однако для RSA сейчас известен только один способ это сделать: найти два простых множителя, составляющих открытый ключ. Поскольку ни один компьютер не в состоянии проделать это в адекватные сроки, RSA считается надежным механизмом обеспечения конфиденциальности.

Некоторые обороты речи, которые я использовал, заслуживают дополнительного объяснения. Для начала я сказал, что ни один компьютер не в состоянии определить простые множители *в адекватные сроки*. Заметьте, я не стал утверждать, что это невозможно в принципе: это возможно. Как уже сказано, если пробовать в качестве делителя каждое простое число по очереди, начиная с 2, в конце концов, два простых множителя будут найдены. Но, учитывая реалии современных компьютерных технологий, человечество успеет вымереть или, по крайней мере, эволюционировать в новый вид, прежде чем подберет все возможные простые множители 900-значного числа[106]. Заметьте, что этот аргумент основан на компьютерах, которые мы используем *сегодня*; чтобы точнее оценить степень безопасности этого алгоритма, необходимо принять во внимание то, какие вычислительные возможности мы ожидаем получить в будущем.

Наверное, еще сильнее тревожит то, что неспособность компьютеров эффективно находить простые множители – не более чем *предположение*. Утверждать, что простые множители сложно вычислить, можно только на основании того, что нам известно; мы не можем учесть неизвестные нам факторы. Более точное утверждение звучало бы так: даже с использованием самых продвинутых современных методик вычисление простых множителей выглядит

сложной задачей. Это не означает, что в будущем какой-то гениальный ребенок или, скажем, искусственный интеллект не разработает новый метод определения простых множителей. Это имело бы катастрофические последствия для любых технологий, в которых используется RSA. Учитывая, сколько всего в киберпространстве защищено этим алгоритмом, такая возможность представляется немыслимой. Но в конце данной книги я все равно попробую поделиться своими мыслями на эту тему.

Зависимость от сложных вычислений

Исходный код нового алгоритма симметричного шифрования, написанный на обратной стороне конверта, вряд ли удовлетворит строгим требованиям безопасности, которые предъявляются к финалисту конкурса AES. И все же он может оказаться не таким уж небезопасным. В связи с этим было предложено множество симметричных и частично блочных шифров. И хотя большинство из них оставляли желать лучшего, существенная часть списка не обнаружила серьезных недостатков, и они доступны для использования, по крайней мере, теоретически[107].

Для сравнения, серьезных алгоритмов асимметричного шифрования до сих пор предложено лишь несколько. Цифровой навесной замок должен иметь свойства, которые могут показаться немного нелогичными. Необходимо разработать вычислительную задачу, которую легко выполнить, но сложно обратить вспять, но при этом она должна быть легко обратимой для того, у кого есть специальный фрагмент информации. Подобных задач известно не так уж много[108].

Впервые концепция асимметричного шифрования возникла в 1970-х годах в двух не связанных между собой организациях: Центре правительственной связи Великобритании (Government Communications Headquarters или GCHQ) и Стэнфордском университете, США. Сначала это открытие, которое в 1990-х могло бы привести к революции в сфере вычислений, произошло в мире спецслужб, но в чисто британском стиле его тихо отложили в сторону.

Интересно, что в обоих случаях изначально появилась лишь *идея* асимметричного шифрования, без примеров алгоритма, и уже позже другие исследователи подхватили эту идею и описали, как ее можно было бы реализовать на практике. Но самое невероятное – то, что и у правительственных исследователей, и у сотрудников университета в результате работы над практическим примером алгоритма асимметричного шифрования получилась фактически одна и та же концепция RSA[109].

Это говорит о двух вещах. Во-первых, найти пример алгоритма асимметричного шифрования действительно непросто. Во-вторых, RSA можно в каком-то смысле назвать «естественным» решением. Процесс поиска простых множителей числа активно изучался математиками на протяжении всей истории, поэтому неудивительно, что именно эта вычислительная задача легла в основу попыток разработать алгоритм асимметричного шифрования. Важную роль сыграло и то, что в этом процессе легко разобраться – это само по себе укрепляет доверие к RSA. По сумме всех факторов RSA, вне всяких сомнений, стал важнейшим алгоритмом асимметричного шифрования на грани двадцатого и двадцать первого веков практически во всех сферах, где нужен этот вид криптографии.

Тем не менее RSA – не единственный алгоритм асимметричного шифрования, с которым вы можете столкнуться. Существует по меньшей мере еще одна распространенная альтернатива, основанная на математической концепции под названием *эллиптические кривые*. Если безопасность RSA опирается на сложность вычисления простых множителей, то в основе эллиптического шифрования лежит сложность операции, известной как *дискретное логарифмирование*[110].

Эта прямая связь с конкретной вычислительной задачей является одновременно и сильной стороной асимметричного шифрования, и источником его слабости. Безопасность блочного шифра можно в какой-то мере сравнить с сооружением замысловатой системы баррикад: для доступа к исходному тексту злоумышленнику нужно вырыть тоннель под стеной, разрезать колючую проволоку, угадать, какой из секретных путей ведет к следующей баррикаде, взобраться на скользкий холм, переплыть ров и пробраться через поле кукурузы в человеческий рост. Чтобы блочный шифр стал еще безопаснее, можно

нагородить еще несколько линий баррикад, пока не появится уверенность в том, что злоумышленник не пройдет.

В то же время безопасность асимметричного шифрования опирается на вычислительную задачу, вокруг которой построен алгоритм. Если эта задача хорошо исследована и, по всеобщему убеждению, действительно сложна (как в случае с поиском простых множителей), соответствующий алгоритм асимметричного шифрования можно уверенно считать безопасным. Но если вдруг вычислительная задача по какой-то причине окажется не настолько сложной, как полагалось, алгоритм обречен. Что-то вроде защитного костюма из материала, который считается пуленепробиваемым. Если он действительно так прочен, вы в порядке. Если нет… что ж, остерегайтесь громких хлопков.

Эта неопределенность в какой-то мере объясняет скептицизм по отношению к новым алгоритмам асимметричного шифрования: они основаны на вычислительных задачах, исследованных не так глубоко и тщательно, как разложение на множители и дискретное логарифмирование. В конце книги я попробую заглянуть в будущее и объясню, почему этот скептицизм нам нужно преодолеть поскорее.

Проблемы с навесными замками

Как вы уже видели, цифровой навесной замок возможен. Асимметричное шифрование позволяет нам обеспечить конфиденциальность соединения между нашим компьютером и сайтом, который мы никогда раньше не посещали. Мы получаем от сайта открытый ключ, который может, к примеру, быть опубликован на его основной странице, и с помощью этого открытого ключа отправляем веб-сайту зашифрованные данные. Блестящее и элегантное решение!

Но не все так гладко. К сожалению, у концепции цифровых навесных замков есть два недостатка, один серьезнее другого. Они, конечно, не делают всю идею бесполезной, но ложку дегтя все-таки добавляют. Подходы, используемые для их компенсации, диктуют способы применения асимметричного шифрования в реальных современных системах.

Первая проблема присуща даже примеру из материального мира, на котором я показал необходимость асимметричного шифрования. Помните юриста и сверхактивного курьера? Я утверждал, что для эффективной передачи юристу бумажного письма сам юрист должен сначала послать вам навесной замок. Здесь есть подвох, о котором я не упомянул. Курьер подъезжает к вашему дому, звонит в дверь и передает вам пакет с навесным замком – все хорошо, но что если курьер окажется мошенником и подменит навесной замок юриста своим собственным? Вы закрываете чемодан с письмом на замок, будучи уверены, что откроет его только юрист. Но, увы, на самом деле ключ к замку есть только у курьера. Проблема в том, что вы не можете быть уверены в подлинности навесного замка, который вам вручают.

Этот сценарий аналогичен получению открытого ключа от сайта. Откуда мы знаем, что это подлинный ключ, предназначенный для взаимодействия с компанией, которая, как вы считаете, владеет этим веб-сайтом? Что, если сайт был взломан? Действительно ли вы ввели правильный адрес, и на самом ли деле он принадлежит компании, с которой, как вам кажется, вы совершаете транзакцию? История киберпреступлений полна примеров того, как невинные пользователи не сумели отличить поддельные веб-сайты от настоящих. Асимметричное шифрование основано на предположении о том, что, прежде чем что-то шифровать, вы получили правильный открытый ключ. Если в этом есть сомнения, идея теряет всякий смысл[111].

Чтобы решить проблему с определением подлинности открытых ключей, нам нужно выработать процедуру, которая позволила бы надежно привязывать их к людям и организациям. Это на удивление сложная задача. Как и многие другие технологии, криптография работает блестяще, пока ею не начинают пользоваться живые люди. Мы можем быть как умными, находчивыми, творческими и готовыми принять новые идеи, так и ленивыми, эгоистичными, манипулятивными и наивными. Создание безопасного навесного замка – это одно, а поиск надежной и честной курьерской службы – совершенно другое. Я вернусь к этому острому вопросу позже, когда речь пойдет о том, как можно нарушить работу криптографии.

Но даже если предположить, что нам удалось с какой-то долей уверенности убедиться в подлинности открытого ключа, остается еще одна проблема, на этот раз техническая. Все алгоритмы

асимметричного шифрования, известные на сегодня, работают медленно. По крайней мере, *медленнее симметричного шифрования*. При шифровании данных с помощью AES задержек почти не возникает, но шифрование с использованием RSA требует определенного времени, хотя вы, скорее всего, даже не заметите разницы. Например, на ноутбуке выполнение алгоритма RSA может занять несколько тысячных долей секунды. Кого это заботит, верно? Но для веб-сайта, заваленного миллионами запросов на установление безопасных соединений, задержка уже может оказаться заметной даже человеку.

Давным-давно никто не обращал внимания на секундные задержки. В Англии 1920-х годов, как описывал ее Лори Ли в своей книге *Сидр с Рози*, героиня с радостью бы запустила шифрование RSA (если бы оно в те времена существовало, и если бы у нее было какое-то устройство, на котором его можно использовать) и пошла бы подоить корову или взбить немного масла, чтобы через час или два получить свой зашифрованный текст[112].

В современном мире секунды имеют значение. Цены на акции поднимаются и падают в мгновение ока. Покупатели бросают виртуальные корзины покупок, если веб-сайт не успевает вовремя ответить. У пассажиров есть лишь несколько мгновений, чтобы пройти через турникет, прежде чем стоящие за ними люди начнут скандалить. Все должно происходить *мгновенно*. Эта жажда скорости особенно относится к таким вещам как шифрование, которое никто на самом деле не *хочет* делать, но которое при этом необходимо. Это означает, что шифрование должно быть очень, очень быстрым.

Лучшее из обоих миров

Симметричное шифрование работает быстро, но у него есть почти нерешаемая проблема с распространением ключей. Асимметричное шифрование медленное, но позволяет загружать ключи прямо с сайтов. У каждого из двух подходов есть положительные стороны, которые удачно дополняют друг друга. Реально ли воспользоваться преимуществами обоих типов шифрования, не пострадав при этом от их недостатков?

Вернемся к нашему любимому примеру и рассмотрим окончательное решение. Курьер доставляет вам навесной замок от юриста. Вы сначала берете обычный ключ (который используется как для закрытия, так и для открытия замка) и закрываете ящик с письмом. Затем вы кладете этот ключ в ящик поменьше и закрываете его на замок, полученный от юриста. Оба ящика курьер передает юристу, который сначала откроет меньший из них, возьмет находящийся в нем ключ и затем откроет большой. Чем сильнее мы усложняем эту аналогию, тем нелепей она становится, поэтому давайте сосредоточимся на веб-сайтах, где это решение выглядит намного логичней.

Эту идею часто называют *гибридным шифрованием*. Допустим, вам нужно установить безопасное конфиденциальное соединение с веб-сайтом. Сначала вы получаете от сайта открытый ключ. Вы бы рады воспользоваться им для шифрования своих данных, но, к сожалению, асимметричное шифрование работает медленно. Поэтому вы генерируете симметричный ключ и быстро шифруете свои данные с его помощью в формате AES. Затем вы шифруете свой симметричный ключ, используя RSA и открытый ключ, полученный от веб-сайта. Эта процедура быстрее не стала, но симметричный ключ размером 128 бит – это очень небольшой фрагмент данных, намного меньше, чем вся та информация, которую вы хотите передать по защищенному каналу. В итоге вы отправляете два зашифрованных элемента. Веб-сайт сначала (медленно) расшифровывает симметричный ключ, а затем использует его, чтобы (быстро) расшифровать данные, зашифрованные с помощью AES. В этой схеме применяются сильные стороны обоих подходов.

В технологиях повседневного применения асимметричное шифрование почти всегда реализовано в виде гибридного процесса. Как уже говорилось, гибридное шифрование, как правило, предназначено для защиты соединений между двумя компьютерами, как в случае с веб-браузером, который подключается к сайту. Не менее активно оно применяется и для защиты электронных писем: симметричный ключ асимметрично шифруется с помощью открытого ключа, принадлежащего адресату, после чего тело письма шифруется с применением симметричного ключа[113].

Это чудо – держитесь подальше!

Асимметричное шифрование кажется чудесным; сложно найти для него более подходящий эпитет. На протяжении столетий криптографам приходилось бороться с проблемой распространения симметричных ключей. Они и представить не могли, что у этой проблемы будет криптографическое решение. Идея цифрового навесного замка действительно совершила революцию, сделав возможным безопасное взаимодействие между незнакомцами. В конце 1990-х асимметричное шифрование позволило обеспечить конфиденциальность для растущего взрывообразно круга неопытных пользователей Всемирной паутины. Можно сказать, что успех Интернета, по крайней мере отчасти, стал возможным благодаря чудесам асимметричного шифрования.

Однако не следует недооценивать две уже названные проблемы, присущие использованию асимметричного шифрования. Надежное привязывание пользователей к их открытым ключам – это *действительно* сложный процесс. И асимметричное шифрование *действительно* медленное. Где-то в 2000 году началось его стремительное падение на знаменитом графике «цикла хайпа»[114] – от «пика чрезмерных ожиданий» к «избавлению от иллюзий». Примерно тогда компании, испытывающие спад после бурного роста доткомов, начали понимать, что асимметричное шифрование – это чудодейственный эликсир с ложкой дегтя. Чего они не понимали, так это того, что асимметричное шифрование даже в гибридном виде имеет смысл использовать только тогда, когда это действительно необходимо.

Основная проблема заключается в следующем: цифровой навесной замок становится действительно необходим только при работе в относительно *открытом* окружении, в котором вы не можете контролировать систему в целом (включая пользователей и сеть, лежащую в основе взаимодействия). Именно это происходит, когда вы просматриваете веб-страницы или отправляете электронные письма в разные уголки планеты. Если же вы работаете в *закрытом окружении*, в котором система находится под вашим контролем, асимметричное шифрование попросту не требуется.

Возьмите любого потребителя технологий шифрования на свой выбор: банки, сотовые операторы, автопроизводители, применяющие электронные ключи, изготовители смарт-карт для проезда в общественном транспорте, создатели контроллеров для беспроводных сетей. Во всех этих примерах кто-то контролирует пользователей системы, используемую сеть, и что важнее всего – процесс распространения симметричных ключей. Если у вас есть возможность контролировать пользователей и спокойно передавать ключи, в асимметричном шифровании нет необходимости. Если вы можете достаточно успешно шифровать данные с помощью одних лишь быстрых симметричных алгоритмов, именно это и следует делать.

Асимметричное шифрование – это инструмент для решения очень специфической задачи: как поделиться секретной информацией с незнакомцем. Решения этой на первый взгляд нерешаемой задачи могут иметь свои недостатки, но важно то, что они находятся в рамках возможного, и их можно использовать, когда (и только!) возникает такая необходимость.

5. Цифровые канарейки

В торым ключевым элементом безопасности, вслед за конфиденциальностью, является *целостность* (или *достоверность*) *данных*, свидетельствующая о том, что информация не изменилась при передаче. В материальном мире вы каждый день полагаетесь на несколько механизмов обеспечения целостности: запечатанные конверты, голограммы на купюрах и т. д. Но при этом вам нужен контекст: вы верите в достоверность выписанных вам лекарств, поскольку они похожи на настоящие, и продал вам их человек, внешне напоминающий фармацевта. В киберпространстве фактор контекста теряет свою надежность, а для обеспечения целостности требуются некоторые инструменты.

Ненадежность данных

Безопасность данных обычно ассоциируют с конфиденциальностью. Поскольку секреты есть у всех, конфиденциальность, как правило, имеет повышенный приоритет. Но оправданно ли это?

Возьмем, к примеру, ваш банковский счет. Сколько бы денег на нем ни было, вам, наверное, не хочется раскрывать свой баланс всем подряд. Если на счету солидная сумма, вас начнут донимать рекламой предметов роскоши, а если нет – предложениями взять кредит, и в любом случае ваш образ жизни начнут обсуждать за вашей спиной. Желание хранить в тайне баланс на банковском счете вполне разумно.

Но что если бы вам пришлось выбирать между сохранением баланса в секрете и гарантией того, что он правильный? Надеюсь, вы никогда не столкнетесь с таким нелепым выбором, но представьте на секунду, что это случилось. Завышенный баланс можно было бы только приветствовать, но смирились бы вы с балансом, который ниже реального?[115]

Даже по сравнению со словами на бумаге данные в компьютерах склонны к случайным повреждениям. Это может произойти в любой

момент. Данные могут непреднамеренно измениться во время их записи или чтения из памяти устройства. Они могут быть повреждены при обработке каким-то приложением или при передаче по сети, особенно беспроводной. Изменения могут произойти даже во время хранения, когда их никто не трогает.

Но, разумеется, еще большее беспокойство вызывает намеренная модификация. Данные очень легко отредактировать. Всего за несколько секунд несанкционированного доступа «цифровой вандал» может посеять хаос в таблице годовых доходов компании или изменить концовку в свежем романе писателя. Осторожное добавление ноля к вашему банковскому балансу может обеспечить вам безоблачное финансовое будущее, но если так же осторожно удалить ноль, ваше благосостояние может потерпеть крах.

Целостность данных – это гарантия того, что они не поменялись с момента их санкционированного создания. Важно понимать, что этот механизм не защищает данные от повреждения: он лишь позволяет с большой долей вероятности определить, были ли они модифицированы тем или иным образом[116]. Механизм обеспечения целостности данных – прежде всего способ предупреждения, как канарейка, падающая замертво со своей жердочки в викторианской угольной шахте[117].

Степени целостности

В силу некоторых нюансов концепция целостности данных не настолько очевидна, как конфиденциальность. В силу тех же особенностей для ее обеспечения разработан целый ряд механизмов безопасности.

Один нюанс состоит в серьезности предполагаемой угрозы: некоторые механизмы распознают только случайные изменения, но не намеренные.

Еще один нюанс заключается в вопросе, распространяется ли целостность данных на их источник, то есть на тех, кто эти данные создал. Такие гарантии кажутся очевидными и неотъемлемыми во многих повседневных ситуациях. Например, при переводе денег вы

ожидаете, что получатель будет уверен в том, что этот перевод сделали вы. Здесь гарантируется, что данные не менялись с момента, когда их санкционированным образом создал *идентифицируемый источник*, а не *кто угодно*. Это более жесткое понятие целостности данных иногда называют *проверкой происхождения*.

Третий нюанс касается сторон, которым эти данные должны быть доступны. Во многих ситуациях вроде обмена файлами между двумя людьми возможность проверить целостность данных нужна только получателю. Однако при подписании цифровых контрактов крайне важно, чтобы целостность данных можно было продемонстрировать третьей стороне – например, судье, который в будущем может улаживать потенциальный конфликт.

Давайте рассмотрим несколько механизмов, обеспечивающих разную степень целостности данных.

Фейковые новости

Стоит отметить, что целостность данных заключается в проверке неизменности информации, но не ее *корректности*.

Разницу можно проиллюстрировать на примере такого явления, как *фейковые новости*[118], когда дезинформация преподносится как факт. Журналисту несложно сфабриковать такую статью и выпустить ее в дикий мир электронных СМИ. Киберпространство – вполне подходящее место для таких фокусов, так как нехватка физического контекста, окружающего новостную статью в Интернете, затрудняет проверку ее правдивости[119]. Фейковая новость может быть ложной, но если читатель получит ее в том виде, в котором она была написана журналистом, можно будет утверждать, что целостность данных сохранена. Механизм целостности данных позволяет читателям определить, вносились ли в статью какие-то изменения с момента ее создания, и в этом смысле, несмотря на свою неправдивость, фейковые новости могут считаться достоверными. Иными словами, читатели получают гарантию того, что статья является такой же ложной, как и в тот день, когда ее написали.

Эта путаница между правдивостью и корректностью возникает из-за отличий между понятиями *целостности* и *честности*[120]. Под честностью обычно понимают «правдивость и сильные моральные качества», чего обычно не хватает в мире фейковых новостей. Честность и моральность – это качества, которые легче оценить человеку, чем компьютеру, следовательно, что криптографические механизмы обеспечения целостности данных для этого малопригодны. С другой стороны, под *целостностью* мы понимаем «состояние неделимости». Именно это понятие я здесь рассматриваю. С помощью криптографии можно определить, остаются ли данные цельными и неделимыми с момента их создания. Это, как ни странно, означает, что криптографию можно использовать для защиты от фейковых новостей, но не для их предотвращения.

Целостность или не целостность, вот в чем вопрос

Чтобы подтвердить цельность и неделимость данных, нам нужен одобренный источник «истины» о том, в каком состоянии должны находиться эти данные. Являются они целостными или нет? Где следует искать ответ на этот вопрос?

Самый очевидный вариант состоит в использовании определенного источника, которому можно довериться при оценке целостности. Если ваш друг что-то говорит, и вы ему доверяете, будет логично предположить, что вы верите в правдивость его слов[121]. Еще один распространенный подход заключается в доверии какого-то рода вышестоящей инстанции. Если вы не уверены, правильно ли пишете какое-то слово, вы можете обратиться к авторитетному источнику, такому как *орфографический словарь*.

В реальности вопросы доверия зачастую менее очевидны. Например, при загрузке программного обеспечения из Интернета на соответствующем веб-сайте нередко можно увидеть так называемый *MD5-хеш*[122]. Это значение позволяет вам убедиться в том, что загруженное вами ПО идентично тому, которое предоставлено на сайте. Этот механизм проверки подлинности работает, только если вы «доверяете» веб-сайту – и не только благим намерениям его авторов,

но и их умению обеспечить кибербезопасность, исключить возможность взлома. Веб-сайт предлагает себя в качестве центра доверия, который гарантирует целостность: «доверять или не доверять – выбор за вами».

Большинство криптографических механизмов для поддержки целостности данных зависят от определенных источников истины. Эти источники, как правило, привязаны к ключам. Чуть позже я объясню, как это работает, на примере нескольких таких инструментов. Но для определения корректности данных можно сверяться не с отдельным источником, а с *всеобщим мнением о нем*.

В 2016 году относительно скромный футбольный клуб «Лестер Сити» выиграл английскую Премьер-лигу, чем немало удивил и экспертов, и почти всех, кто мало-мальски интересуется спортом. Но как мы можем быть *уверены* в том, что это действительно произошло, если мы не присутствовали на стадионе, когда игрокам «Лестер Сити» вручали кубок? Стоит ли считать это правдой только потому, что об этом написали в газете или показали по телевизору? Или потому, что об этом рассказал приятель? Может, стоит обратиться непосредственно в английскую Премьер-лигу и потребовать письменного подтверждения? Большинство людей верит в то, что «Лестер Сити» стал чемпионом, потому что об этом твердят все вокруг. Для оценки правдивости этой информации мы полагаемся не на конкретный источник, а на тот факт, что все доступные нам источники с ней согласны. «Лестер Сити» выиграл, потому что так считает весь мир.

По ряду причин в наши дни наблюдается рост интереса к механизмам обеспечения целостности, которые используют более глобальные ориентиры. Это касается, помимо прочего, таких технологий как Bitcoin (об этом чуть позже), которые обеспечивают целостность цифровой валюты, не прибегая к услугам какого-то одного надежного банка.

Проверка целостности

Чтобы проверить корректность информации, можно попробовать найти ее подтверждение. Для определения правдивости показаний в суде обычно стараются получить информацию из разных источников,

сверить и установить, какие ее аспекты не вызывают сомнений. Для определения корректности экспериментальных результатов ученые проводят эксперименты заново. В идеале, чтобы сформировать мнение о целостности любых данных, мы оцениваем свидетельства, полученные из разных источников, каждому из которых мы доверяем в той или иной степени.

Однако во многих ситуациях мы не можем позволить себе роскошь поиска вспомогательных свидетельств. Когда наш браузер уже взаимодействует с интернет-магазином, нам не к кому обратиться за оценкой целостности и достоверности данных, которыми они обмениваются. Решение о том, доверять этим данным или нет, нужно принимать немедленно, исходя из текущего сеанса взаимодействия, причем эффективно и без задержек.

Задумайтесь на секунду, как вы подходите к этой проблеме в материальном мире. Возьмем в качестве важной письменной информации, целостность которой должна быть гарантирована, графу об образовании соискателя на какую-то должность. В исключительных обстоятельствах потенциальный работодатель может лично позвонить преподавателям кандидата, чтобы подтвердить достоверность сведений из анкеты, но обычно такой способ проверки неэффективен.

Вместо этого обычно смотрят, есть ли в документах соискателя официальная печать, реальное назначение которой – косвенно продемонстрировать, что *достоверность информации, изложенной на этом листе бумаги, подтверждается автором печати*[123]. Сама печать не занимает много места и несет в себе намного меньше информации, чем документ, но вместе с тем она выступает гарантией правдивости всего документа. Работодателю достаточно проверить только саму печать, и, удовлетворившись результатом этой проверки, он может исходить из того, что вся остальная информация в документе тоже, скорее всего, верна.

Существует много других ситуаций, в которых крошечный, поддающийся проверке фрагмент информации выступает гарантией целостности и достоверности более крупного объема данных. Пожалуй, самым распространенным средством подтверждения подлинности является подпись от руки. Интересно, что подписи используются в нескольких разных контекстах безопасности, но чаще всего с их помощью гарантируют корректность документа.

Подписывая письмо или договор, вы тем самым подтверждаете свою удовлетворенность достоверностью изложенной там информации. Любой, кто ссылается на подписанный документ, предполагает, что вы как подписант были согласны с его содержимым в момент подписания.

Печати и подписи от руки можно считать компактными знаками одобрения достоверности письменного документа. Однако их эффективность зависит от материальности того, что они подтверждают. Недобросовестный кандидат может попытаться подделать сведения о своей академической успеваемости в надежде, что потенциальный работодатель не обратит на это внимания. Точно так же мошенник может подписать письмо и позже изменить его содержание. К сожалению, для борьбы с такими подделками пока не придумали ничего, кроме обременительных правовых процедур, таких как хранение копий договоров в офисе юриста.

Но основная проблема компактных гарантий целостности, таких как печати и подписи, состоит в их статичности: они не меняются с момента проставления. Печать на документе остается без изменений независимо от того, был ли он изменен мошенником. После подписания письма его могут исправить сколько угодно раз. Действительно, в материальном мире сложно себе представить, что к этой проблеме можно было бы подойти иначе. Это одна из причин, почему контекст играет такую важную роль в обеспечении достоверности в повседневной жизни.

Цифровой мир дает возможность выработать намного лучшее решение. Информация в нем представлена в виде чисел. И, поскольку числа можно комбинировать и вычислять, мы можем сделать то, что в материальном мире невообразимо: разработать средства обеспечения целостности, которые, помимо компактности и простоты проверки, *зависят от самих данных*. Иными словами, мы можем поставить на документ цифровую печать, которая перестанет быть действительной при внесении в этот документ любых изменений. Взамен на физическую и контекстную целостность киберпространство предлагает механизмы, сложность и утонченность которых недоступна в материальном мире.

Злой библиотекарь

Давайте начнем с простого механизма обеспечения целостности данных, рассчитанного на информацию, состоящую из чисел. *Международный стандартный номер книги* (International Standard Book Number, ISBN) – это общепризнанное средство однозначной идентификации изданных книг (вы можете найти его на обложке этого издания)[124]. Например, однозначно достойная прочтения книга *Dachshunds for Dummies* Ив Адамсон (John Wiley, 2007) имеет ISBN 978–0-470–22968-2. Ее можно точно идентифицировать по этому номеру. Если кто-то решит написать книгу с тем же названием, у нее будет другой ISBN. Этот механизм особенно полезен для библиотекарей и книготорговцев, которые благодаря ему могут быть уверены, что имеют дело с нужным изданием.

Тем не менее нам намного легче выговорить или набрать на клавиатуре название книги, чем нечто вроде «978–0-470–22968-2». Если вы допустите ошибку в слове *dachshund*, большинство компьютерных систем проверки орфографии автоматически ее исправят. С опечаткой в номере 978–0-470–22968-2 вам вряд ли так повезет. В связи с этим в каждый номер ISBN встроена проверка целостности, чтобы с достаточно высокой вероятностью выявить ошибки и опечатки. Первые двенадцать цифр составляют уникальный серийный номер, а для проверки их корректности используется последняя, *контрольная цифра*. Она вычисляется простым способом: цифры в позициях 1, 3, 5, 7, 9 и 11 прибавляются к сумме цифр в позициях 2, 4, 6, 8, 10 и 12, умноженной на 3; затем последняя цифра полученного результата вычитается из 10. То, что получилось, становится тринадцатой цифрой в ISBN. В нашем примере ($9 + 8 + 4 + 0 + 2 + 6 = 29$) прибавляется к $3 \times (7 + 0 + 7 + 2 + 9 + 8 = 33)$, а из результата (128) берется последняя цифра (8) и вычитается из 10. Получается 2.

Тринадцатая цифра может автоматически вычисляться каждый раз, когда ISBN вводится в компьютер. Если в какой-либо из первых двенадцати цифр произошла ошибка, результат вычисления с высокой степенью вероятности не совпадет с последней цифрой в ISBN. Если вместо четвертой цифры в нашем примере (0) случайно ввели 1 (в результате чего получился номер 978–1–47–968-2), вычисление контрольной цифры вернет 9. Поскольку тринадцатая цифра должна быть равна 2, это свидетельствует об ошибке. Есть риск, что

контрольная цифра все равно будет вычислена правильно (например, если в нашем номере ISBN было сделано две опечатки, 978–1-470–22968-9), и что ошибка останется незамеченной, но в большинстве случаев несоответствие удается выявить.

Необходимо понимать, что номер ISBN не рассчитан на борьбу с намеренными ошибками. У этого механизма не предусмотрено никакой защиты на случай, если библиотекарь-манипулятор сознательно решит внести в ISBN какие-то изменения. Предположим, что он поменял в нашем примере двенадцатую цифру ISBN с 8 на 7. Если это единственное изменение, номер 978–0-470–22967-2 будет помечен как некорректный ввиду несовпадения контрольной цифры. Однако определить, какой должна быть тринадцатая цифра, может кто угодно, так что нашему злому библиотекарю достаточно подобрать подходящее значение для номера 978–0-470–22967. 29 плюс 3 × 32 равно 125; берем последнюю цифру (5) и получаем 10 – 5 = 5. Таким образом, чтобы избежать разоблачения, библиотекарь должен поменять контрольную цифру на 5. В результате получится корректный номер ISBN 978–0-470–22967-5, который по случайному стечению обстоятельств принадлежит родственному изданию *Chihuahuas for Dummies* (поэтому даже не надейтесь, что такая ужасная манипуляция останется незамеченной).

Как мы все знаем, библиотекари обычно не злые. ISBN обеспечен очень скромным механизмом проверки целостности исключительно для предотвращения случайных ошибок. Тем не менее мы полагаемся на номера, по смыслу близкие к ISBN, во многих аспектах нашей жизни, и наличие в них простой проверки целостности лучше, чем ничего. Контрольные цифры, которые вычисляются аналогичным образом, присутствуют в номерах кредитных карт, номерах социального страхования и системе нумерации европейских локомотивов[125].

На пути к более строгой проверке целостности

Контрольная цифра, интегрированная в ISBN, – крайне простой предохранитель. Однако подобные механизмы проверки целостности

имеют нечто общее с более строгими криптографическими средствами, о которых стоит упомянуть.

Важнее всего то, что контрольные цифры, в отличие от печатей на физических документах, служат компактной гарантией защиты информации, поскольку *они из нее вычисляются*. У каждого отдельного элемента данных, такого как книжный номер, может быть только одна правильная контрольная цифра. Но, поскольку потенциальных контрольных цифр всего десять, намного меньше, чем самих книг, мы имеем дело с множеством номеров ISBN с одинаковыми контрольными цифрами, и ничего не можем с этим сделать. Это нельзя назвать проблемой как таковой, но из-за этого мы можем не обнаружить некорректный ISBN, так как контрольная цифра неправильного номера может быть вычислена по всем правилам. Риск такого совпадения можно было бы снизить за счет проведения дополнительной проверки, но за это пришлось бы заплатить ухудшением эффективности (в данном случае номер ISBN пришлось бы сделать длиннее). Криптографические механизмы обеспечения целостности тоже иногда допускают подобный компромисс между эффективностью и безопасностью.

Следует подчеркнуть, контрольные цифры не *гарантируют* обнаружение ошибок; они лишь позволяют их обнаруживать с предсказуемой вероятностью. Возникновение этих ошибок они тоже не предотвращают (на самом деле ни один механизм, основанный исключительно на вычислении данных, на это не способен), да и исправлять их не способны. Все это в той же степени относится и к криптографическим механизмам обеспечения целостности.

К сожалению, одно из ключевых свойств контрольных цифр крайне нежелательно для более строгих криптографических механизмов. Контрольная цифра в ISBN вычисляется путем простого сложения и умножения первых двенадцати цифр, поэтому предсказать, как изменение основной части ISBN отразится на значении контрольной цифры, довольно легко. Это означает, что мы можем предсказать контрольную цифру при изменении одного из элементов ISBN или сложении двух ISBN вместе, и тем более определить, контрольные цифры каких номеров ISBN совпадут.

Тем не менее книготорговцев и библиотекарей не заботит предсказуемость контрольных цифр, и никому и в голову не придет

складывать разные номера социального страхования. В этих примерах контрольные цифры работают достаточно хорошо.

Швейцарский армейский нож мира криптографии

Контрольные цифры для проверки целостности – это инструмент с ограниченными возможностями. Если вам нужно что-то более серьезное, и вы готовы заплатить за это повышенной сложностью реализации и снижением производительности, вам стоит воспользоваться криптографической *хеш-функцией*[126].

Хеш-функция принимает данные любой длины и возвращает для них короткую проверку целостности – собственно *хеш*, – не задействуя никакие ключи, что немного необычно для криптографического инструмента. Хеш, как и контрольная цифра, намного меньше самих данных, из которых его вычисляют. Если нам, к примеру, нужно определить, изменился ли файл за время передачи по сети, можно предварительно вычислить его хеш и послать его получателю вместе с файлом. Чтобы убедиться в целостности пришедшего файла, получатель вычисляет его хеш, сравнивает с присланным, и если они совпадают, может заключить, что файл в пути не изменился.

Чем хеш отличается от контрольной цифры, так это способом получения. Если контрольная цифра выводится из данных предельно просто, то хеш вычисляется с помощью криптографического алгоритма. Вспомните, как я ранее сравнивал криптографические алгоритмы с миксерами. Эта аналогия хорошо подходит для шифрования, поскольку соответствующий алгоритм смешивает набор ингредиентов без изменения их общей массы, иными словами, зашифрованный текст является рандомизированной версией исходного, но имеет (примерно) ту же длину. Функция хеширования тоже смешивает исходные данные, но ее вывод намного меньше ввода. Она больше похожа на соковыжималку: ингредиенты измельчаются, но то, что из нее выходит, по объему намного меньше того, что мы в нее положили.

Основное преимущество хеша перед контрольными цифрами в том, что криптографический процесс, применяемый для его вычисления, скрывает связь между ним и исходными данными. В отличие от

контрольной цифры, при любом изменении в данных хеш меняется непредсказуемо. Даже если поменять в файле один бит информации, итоговый хеш не будет иметь никакой видимой связи с хешем оригинального файла. Кроме того, найти два файла, у которых совпадал бы хеш, чрезвычайно сложно, чего нельзя сказать о контрольных цифрах.

Возможно, это прозвучит неожиданно, но хеш-функции – один из полезнейших когда-либо придуманных криптографических инструментов[127]. В отличие от алгоритмов шифрования, они мало что могут сами по себе, но в качестве вспомогательного средства для более сложных криптографических операций они незаменимы. Собственно, именно поэтому их нередко называют «швейцарским армейским ножом» мира криптографии.

Начнем с того, что их можно применять как связующее звено между разными элементами данных. Поскольку хеши, в сущности, непредсказуемы, с помощью хеш-функций можно генерировать случайные числа. Ввиду способности сжимать данные хеш-функции хороши как основа других криптографических механизмов, например, цифровых подписей, повышая их эффективность. Еще один способ их использования – защита паролей. Система криптовалюты Bitcoin тоже основана на разностороннем применении хешей, следовательно, хеш-функции способствуют развитию экономики неконтролируемой части глобальной сети (Dark Web).

О каждом из трех последних сценариев мы поговорим чуть позже.

Целостность перед лицом злого умысла

К сожалению, хеш-функция сама по себе не обеспечивает целостность в ситуации, когда злоумышленник может намеренно изменить данные. Библиотекарь вряд ли извлечет какую-то выгоду из манипуляции контрольными цифрами ISBN, но нельзя сказать того же о злоумышленнике, который наблюдает за отправкой файла и его хеша через Интернет. Если он захочет изменить файл и остаться незамеченным, ему достаточно после внесения изменений вычислить и отправить новый хеш: когда адресат получит модифицированный файл, хеш успешно пройдет проверку. Это объясняется тем, что хеш

данных, как и контрольную цифру в номере ISBN, может вычислить любой.

С этой проблемой можно бороться двумя путями. Во-первых, можно передать хеш получателю средствами, которыми злоумышленник неспособен манипулировать. Например, можно послать другу файл по электронной почте, а хеш продиктовать по телефону: поскольку хеш достаточно короткий, это достаточно легко. Дальше остается только сверить хеш полученного файла с тем, который вы сообщили.

Но зачастую использовать те или иные средства защиты хеша невозможно или как минимум неудобно. В таких случаях концепцию хеш-функций необходимо адаптировать так, чтобы хеш данных не мог вычислить кто угодно. К счастью, этого можно добиться довольно очевидным способом. Как вы помните, хеш-функция – это криптографический алгоритм, который просто сжимает данные в хеш меньшего размера *без использования ключа*. Таким образом, чтобы ограничить круг тех, кто может вычислить хеш, в процесс его вычисления достаточно как-то интегрировать ключ.

О происхождении данных

Итак, следующим этапом улучшения нашего механизма обеспечения целостности становится *хеш-функция с ключом*. Представьте, что вы согласовали со своим другом секретный криптографический ключ. Вы добавили его в файл и вычислили хеш из того, что получилось. Затем вы отправили другу файл без ключа, но с хешем. Он добавил в файл ваш согласованный ключ и вычислил хеш заново. Если этот хеш совпал с присланным, ваш друг может быть уверен в том, что файл не изменялся.

Такая комбинация должна защитить файл от намеренных изменений. Злоумышленник может перехватить файл во время передачи и внести в него любые изменения. Но после этого ему не удастся вычислить корректный хеш. Ему известно содержимое измененного файла, но у него нет ключа, поэтому хеш их сочетания останется неизвестным. В результате любые изменения, внесенные в файл, будут обнаружены.

Это, в сущности, превосходная идея. Но по многим техническим причинам, которыми я не стану вас утомлять, она не слишком практична[128]. В реальности используются специальные хеш-функции, которые встраивают секретный ключ более сложным образом, чем прямое добавление к данным. Их обычно называют *имитовставками* (или *кодами аутентификации сообщений* – англ. message authentication codes или MAC). Один из популярнейших алгоритмов MAC называется *HMAC*[129] и основан непосредственно на хеш-функции («H» от слова «hash»). Существуют и другие; например, *CMAC*[130] основан на блочном шифре («C» от слова «cipher»).

Имитовставки – это один из важнейших криптографических механизмов для защиты повседневной деятельности в киберпространстве. Их полезность объясняется тем, что наличие ключа позволяет не только защититься от злоумышленников, которые намеренно манипулируют данными, но и повысить уровень обеспечения целостности, что делает возможной проверку подлинности происхождения данных, с которой вы познакомились ранее. Если мы успешно проверяем имитовставку полученного файла, ключ подтверждает его источник. Тот, кто вычислил имитовставку, должен обладать ключом, и получатель знает, что помимо него этот ключ известен только отправителю. Следовательно, файл не мог прийти ни от кого другого.

Вне всякого сомнения, вы неоднократно использовали имитовставки, сами того не осознавая. Они обеспечивают проверку происхождения (и, следовательно, целостность) банковских транзакций, операций с платежными картами, взаимодействий по Wi-Fi, безопасных веб-соединений и многого другого. Симметричное шифрование данных без применения имитовставок встречается нечасто. Конфиденциальность и проверка происхождения идут рука об руку настолько часто, что для блочных шифров был предложен целый ряд режимов работы с *аутентификацией шифрования*, которые позволяют одновременно зашифровать данные и вычислить их имитовставку. Эти режимы становятся все популярней, и в будущем их, вероятно, будут предлагать по умолчанию[131].

То, что может сделать один, под силу другому

Если говорить о надежном средстве обеспечения целостности данных в виде проверки происхождения, имитовставки кажутся идеальным вариантом. Они способны обнаружить малейшие изменения, случайные или намеренные; с их помощью можно определить источник данных; они широко применяются во многих важнейших областях прикладной криптографии. Что может быть лучше?

Имитовставка дает получателю гарантию того, что файл не изменялся. Для большинства реальных задач этой гарантии должно быть достаточно. И все же это не самое надежное средство проверки происхождения данных. Чтобы понять, почему, задайтесь следующим вопросом: может ли *кто угодно*, используя имитовставку, удостовериться в том, что файл пришел от заданного отправителя и не был модифицирован?

Рассмотрим применение имитовставки для защиты цифрового договора, отправленного по Интернету. Получатель может быть уверен в том, что договор пришел от определенного отправителя. Но что если позже у отправителя и получателя возникнет спор относительно договора? Если они пригласят для урегулирования конфликта третью сторону, получатель может предоставить имитовставку в качестве доказательства того, что отправитель послал этот договор и тем самым согласился с его условиями. В то же время отправитель может все отрицать, заявив, что получатель сам создал договор и соответствующую имитовставку без его участия. Эта проблема возникает из-за симметричности возможностей отправителя и получателя. Третья сторона, конечно же, может установить, что файл пришел от владельца имитовставки. Но от кого именно? Кто создал имитовставку – получатель или отправитель? Ее мог вычислить любой из них, так как ключ имеется у обоих[132].

Этот пример демонстрирует, что при проверке происхождения данных с помощью симметричной криптографии неизбежно возникают проблемы. В нашем случае симметричный ключ используется совместно отправителем и получателем, поэтому то, что может сделать один, под силу и другому. Следовательно, получатель может подтвердить, что файл прошел от отправителя, но никто другой не может быть в этом уверен, и имитовставка здесь не поможет.

Таким образом, имитовставки – это отличный криптографический механизм для проверки происхождения данных, если только вам не нужно продемонстрировать подлинность происхождения кому-то другому. Если же такая необходимость возникает, в процесс использования ключей при вычислении имитовставок нужно привнести какую-то асимметричность, чтобы их мог создавать кто-то один. Впрочем, вы уже наслышаны о асимметричных ключах, не так ли?

Цифровые навесные антизамки

У большинства физических механизмов обеспечения целостности есть одно свойство, которого недостает контрольным цифрам, хеш-функциям и имитовставкам. Официальная печать на документе или подпись на договоре, возможно, и не помешает внести изменения в их содержание, но оба эти средства служат неоспоримым доказательством авторства. Печать на справке об успеваемости надежно связывает ее с выдавшим ее учреждением. Подпись на договоре фактически говорит о том, что «здесь был подписант». Для сравнения: хеш может вычислить кто угодно, и любой обладатель симметричного ключа может создать имитовставку.

Возможность связать проверку целостности с уникальным источником иногда называют *неподдельностью*, поскольку автор проверки не может отрицать, что он ее инициировал. Неподдельность – это обеспечение целостности данных высшего сорта; она необходима в двух случаях: когда злоумышленник способен манипулировать данными, и когда происхождение данных нужно доказать третьей стороне. Это строгие требования, обуславливающие необходимость мощного криптографического инструмента.

Неподдельность требует наличия криптографического механизма, выполняющего проверку целостности, результат которой уникальным образом связан с ее инициатором. Если вдуматься, то это почти полная противоположность навесному замку. Как вы помните, навесной замок может закрыть кто угодно, но для его открытия необходим ключ. Нам же нужен своего рода «антизамок», который позволяет инициировать

проверку целостности только владельцу ключа, но в подлинности ее результатов может убедиться кто угодно.

Может ли пригодиться знание того, как устроены цифровые навесные замки при создании цифровых антизамков? К счастью, да. Концепцию цифровых навесных замков, основанную на асимметричном шифровании, можно адаптировать для разработки криптографических механизмов обеспечения неподдельности. Этот механизм привязывает данные к уникальному источнику подобно тому, как это делает подпись, поставленная от руки, поэтому он называется *цифровой подписью*.

Цифровые подписи

Принцип работы цифровой подписи представляет собой методы асимметричного шифрования *наоборот*: роли открытого и закрытого ключей меняются на противоположные. При асимметричном шифровании отправитель шифрует свои данные с помощью общедоступного открытого ключа, принадлежащего получателю, который, в свою очередь, расшифровывает их, используя закрытый ключ; следует подчеркнуть, что получатель – единственный, кто имеет доступ к этому закрытому ключу. Чтобы создать цифровую подпись, отправитель *шифрует* данные с помощью закрытого ключа, а его открытый ключ используется получателем для их *расшифровки* и проверки их целостности. Цифровую подпись может проверить кто угодно, так как для этого достаточно открытого ключа отправителя, который тайны не составляет. По крайней мере так это выглядит в теории.

На практике не все так просто. В частности, большинство алгоритмов асимметричного шифрования могут работать в обратном направлении только после небольшой модификации. Но важнее всего, пожалуй, то, что цифровые подписи – это проверка целостности, не предназначенная для обеспечения конфиденциальности. Поскольку данные не являются секретными, логично предположить, что тот, кому нужно проверить подпись, имеет доступ и к самим данным. Соответственно, результат проверки целостности должен передаваться вместе с исходными данными, так же, как подпись служит

дополнением к документу. Если бы для создания подписи данные просто «шифровались», она представляла бы собой шифротекст того же размера, что и сами данные, что сделало бы ее громоздкой и неэффективной по сравнению с компактными контрольными цифрами, хеш-функциями и имитовставками[133].

Ключевой момент здесь в том, что для создания цифровой подписи необязательно «шифровать» (или, если выражаться точнее, *подписывать*) все данные. Достаточно подписать их компактное представление – что-то небольшое, но зависящее от каждого бита данных. Внимательные читатели должны помнить, что у нас для этого есть замечательный инструмент! Обычно для создания цифровой подписи из данных сначала «выжимают» хеш, и уже его подписывают с помощью закрытого ключа отправителя. Любой желающий проверить цифровую подпись может сначала вычислить хеш данных, а затем сравнить его с результатом «расшифровки» (назовем это *проверкой подлинности*) подписи. Если они совпадают, то проверяющий узнает несколько фактов.

Рассмотрим их по очереди.

Первое: уверенность в целостности данных. Если кто-то модифицировал файл, хеш будет отличаться. Злоумышленник, скорее всего, будет способен вычислить этот хеш, но создать на его основе новую цифровую подпись не сможет, не имея доступа к закрытому ключу изначального отправителя.

Второе: уверенность в происхождении данных. Цифровую подпись можно «расшифровать» с помощью открытого ключа отправителя в корректный хеш только в том случае, если для ее создания использовался соответствующий закрытый ключ.

Третье: неподдельность. Цифровую подпись может проверить любой, поскольку для этого достаточно открытого ключа отправителя. Важно, что отправитель не может отрицать факт подписания, так как только ему известен закрытый ключ, соответствующий открытому ключу, с помощью которого проверена подпись.

Гейм, сет и матч.

Цифровые подписи – это первосортный механизм обеспечения целостности; ничто не может соперничать с ними по уровню устойчивости. Но за качественные вещи приходится платить. Надеюсь, вы уже заметили, что цифровым подписям свойственны те же

недостатки, что и асимметричному шифрованию. Во-первых, у нас возникает проблема с определением подлинности открытых ключей (в данном случае – открытых проверочных ключей). Во-вторых, вычисление цифровых подписей работает медленнее, чем другие механизмы обеспечения целостности данных, так как по принципу своей работы оно похоже на асимметричное шифрование.

Если вам не нужен высочайший уровень целостности, который обеспечивают цифровые подписи, их лучше не использовать. Как я уже отмечал, для большинства повседневных криптографических задач достаточно имитовставок. Можно сказать, что цифровые подписи имеют такое же отношение к целостности, как асимметричное шифрование к конфиденциальности. Оба эти механизма обычно требуются в открытых окружениях одного рода. Например, самые безопасные системы электронной почты позволяют шифровать письма с помощью гибридных методов и/или подписывать их. А в домашней беспроводной сети используются симметричное шифрование и имитовставки, поскольку это закрытое окружение, в котором легко обмениваться ключами.

Как ни странно, одно из важнейших направлений использования цифровых подписей состоит в борьбе с их главным недостатком! Цифровые подписи – важный элемент самого распространенного метода проверки открытых ключей, которые применяются как в асимметричном шифровании, так и в самих цифровых подписях. Впрочем, и об этом подробнее поговорим позже.

Отличие цифровых подписей от обычных

Термин *цифровая подпись* создает в нашем воображении образ некой футуристической кибер-руки, которая подписывает цифровые данные. Это подталкивает нас к тому, чтобы считать их эквивалентом подписей, которые ставятся от руки на бумажных документах, только в киберпространстве. Заманчивая, но коварная аналогия. Цифровые подписи действительно имеют некое сходство с обычными, но, несмотря на это, являются чем-то совершенно иным. Называть их *механизмами неподдельности* было бы точнее, но как же скучно это звучало бы!

Цифровые подписи во многих отношениях превосходят обычные. Их главное преимущество, несомненно, в том, что они вычисляются непосредственно на основе исходных данных. Если данные как угодно меняются, цифровая подпись меняется вместе с ними. Следовательно, *каждая версия* документа имеет свою уникальную подпись. Конечно, когда мы расписываемся, чтобы подтвердить курьерскую доставку, мы выводим нашу подпись не так старательно, как при оформлении паспорта, но в целом эти отличия несущественны.

Еще одно ценное свойство цифровых подписей состоит в том, что их можно воссоздать с абсолютной точностью. Если снова подписать те же данные с помощью того же ключа, получится та же цифровая подпись. Потенциально это может даже служить доказательством в суде. Подписи, поставленные от руки, такой точностью не обладают, и порой для подтверждения соответствия двух подписей не обойтись без специалиста.

Однако у цифровых подписей есть и недостатки. Самым важным, пожалуй, можно назвать их зависимость от криптографической инфраструктуры, что означает необходимость хороших методов управления ключами и надежных технологий. Если у этой потенциально недешевой инфраструктуры обнаружится слабая сторона, цифровые подписи потеряют свою эффективность. Например, если кому-то удастся похитить ваш ключ, этот вор сможет создавать цифровые подписи, по всем внешним признакам неотличимые от ваших. Обычные подписи, которые ставятся от руки, не нуждаются в такой инфраструктуре и являются переносимыми в прямом смысле этого слова[134].

Мудрость толпы

Пришло время еще раз задуматься над тем, на кого или на что мы полагаемся при определении целостности данных. Корректны ли данные, что может помочь с ответом? Мы можем подтвердить хеш MD5 загруженного файла, сверив его с тем, который опубликован на сайте. Эта проверка работает, если мы доверяем сайту. Мы можем проверить имитовставку для полученного файла, вычислив ее локально. Это тоже работает, если исходить из того, что отправитель

обладает единственной копией ключа, использованного для вычисления имитовставки. Мы можем проверить цифровую подпись в электронном письме, применив к ней соответствующий проверочный ключ. Но для этого мы должны быть уверены, что открытый проверочный ключ действительно принадлежит отправителю письма.

Во всех этих примерах требуется доверие к конкретным процессам. Эффективность хеша MD5 требует уверенности в реализации сайта и управлении им. Имитовставка требует уверенности в распространении и секретности соответствующих ключей. Цифровая подпись требует уверенности в секретности закрытых ключей и подлинности открытых. Что делать, если нам недостает такого рода доверия?

Один из вариантов, который я описал ранее, говоря о годе славы «Лестер Сити», – довериться *всеобщему* мнению. Если *все* говорят, что информация корректная, мы можем ей доверять. Но этот подход требует определенной осторожности, поскольку во многом зависит от того, кто эти «все».

Граждане Северной Кореи, к примеру, находятся в условиях строгого контроля за информацией. У них очень мало контактов с внешним миром, а их возможность свободно обмениваться информацией друг с другом подавляется за счет надзора за прессой, слежки и ограничений на передвижение. Кроме того, они обязаны слушать ежедневные радиопередачи правящего режима. В результате всех этих мер они без тени сомнения верят во многие вещи, которые большинство из нас правдой не посчитает, поскольку «общественный договор» северокорейского социума представляет собой результат жесткого контроля за информацией со стороны их политического руководства[135].

То, что передается по северокорейскому радио, может не всегда соответствовать фактам, но, поскольку правительство контролирует распространение информации в пределах государственных границ, политические заявления, которые слышат граждане Северной Кореи, подлинны в том смысле, что до людей доходит та информация, которая для них предназначена. Тот факт, что все слышат одно и то же, и большинство граждан этому верит, укрепляет уверенность в достоверности услышанного. Но, как мы отмечали при обсуждении фейковых новостей, *правда* – это совсем другое дело.

Но и более демократичные, нежели Северная Корея, общества не всегда находятся в удачном положении для оценки корректности той или иной информации. Как известно, традиционные СМИ, социальные сети и поисковые системы создают так называемые *пузыри фильтров*, когда получение одних и тех же сведений из разных источников влияет на картину мира пользователя[136]. Несложно поверить в достоверность какой-то информации, если «все» считают ее правдивой, или, по крайней мере, так выглядит. Однако в этих примерах понятие «все» зачастую ограничено так, что пользователь этого не видит или не понимает. Читатели отдельно взятой газеты часто придерживаются одних и тех же политических взглядов; социальные сети самоизбирательны, поскольку большинство людей выбирают себе в друзья тех, с кем имеют общие интересы; поисковые системы основаны на алгоритмах, зависящих от предыдущих действий пользователя (что он искал, какие веб-страницы посещал и т. д.). В этих случаях за понятием «все» может скрываться всего несколько человек, которые, вероятно, не отражают мнения всего общества.

Еще один интересный пример – Википедия. То, что вы прочитали на Википедии, должно быть правдой, верно? Некоторые насмехаются над самой идеей того, что кто-то может доверять этому сайту, считать его истиной в последней инстанции. Следует понимать, что практически кто угодно может создать или отредактировать страницу на Википедии. Информация в ней со временем изменяется, и для этого разработан процесс, в рамках которого пользователи читают, оспаривают и исправляют статьи. Таким образом можно утверждать, что страница на Википедии в конечном счете отражает «общепринятый» взгляд на вещи. Но слабость этого аргумента в том, что некоторые статьи активно изучаются, а в другие редко кто заглядывает, так что понятия «все» и «общепринятый» могут кардинально разниться в зависимости от конкретной страницы. Так что и качество информации, представленной на Википедии, существенно варьируется[137].

Предполагаемая мудрость толпы, как мы уже знаем, имеет свои нюансы. Правдивость информации во многом зависит от того, о какой толпе идет речь. Тем не менее в условиях отсутствия единого центра доверия, на который можно было бы положиться при оценке достоверности, идея использования глобального ориентира выглядит

крайне убедительной. Кто-то сомневается, что Париж – столица Франции?

«Всеобщий» энтузиазм касательно той или иной информации не всегда означает, что ее правдивость будет признана глобально. И ждать месяцы и годы, пока укрепится представление о достоверности каких-то сведений, как в случае со статьями на Википедии, мы обычно тоже не можем. Как же применить эту концепцию глобального ориентира для обеспечения достоверности повседневной информации, такой как, к примеру, количество биткоинов в вашем кошельке? Где найти толпу, мудрости которой всегда можно доверять?

Сам себе банк

Сколько денег на вашем банковском счету? Не нужно отвечать! Просто подумайте о том, как вы определяете корректность этой суммы (будь она положительная или отрицательная). Откуда вы на самом деле знаете, какой у вас баланс? Нравится вам это или нет, ответ на этот вопрос сводится к необходимости доверять своему банку. Именно банк – авторитетный источник вашего баланса. Вы можете не соглашаться с деталями, но говоря откровенно, если вы ему не доверяете, вам стоит перевести свои деньги куда-то еще[138].

Однако для некоторых типов информации может не существовать единого авторитетного и одновременно доверенного источника. Или же мы не *хотим*, чтобы такой центр доверия существовал. Возьмем, к примеру, систему цифровой валюты Bitcoin[139]. Ее основное назначение – имитировать ту свободу действий, которую мы предполагаем для наличных денег, в том числе отсутствие необходимости взаимодействий с банком и относительная анонимность производимых транзакций. Цифровые деньги могут быть обеспечены единым центральным банком, но в таком случае этому банку должны доверять все пользователи[140]. Альтернативное решение, которое применяется в Bitcoin, – имитировать роль банка, не прибегая к его услугам.

Для чего нужен банк, если уж на то пошло? В том, что касается валютных операций, его важнейшая роль – служить доверенной

стороной, наблюдающей за вашими входящими и исходящими транзакциями, неоспоримым источником истины касательно достоверности баланса на вашем счету. Банку непросто заслужить такое доверие; для получения достаточного авторитета необходимо много работать. Он должен заниматься разными взаимосвязанными видами деятельности, включая продвижение своего бренда, соблюдение финансовых норм, проведение финансового аудита, работу с персоналом и использование многочисленных физических и цифровых средств безопасности (банки – заядлые пользователи криптографии)[141]. Все это в совокупности защищает финансовую информацию, надзор за которой доверен банку. Эту информацию можно считать своего рода *централизованной бухгалтерской книгой*, содержащей сведения о финансовых операциях всех клиентов, перед которыми банк ответственен.

Если мы не хотим, чтобы банк надзирал за нашими транзакциями, кто будет этим заниматься? Ответ прост: «все». Идея *распределенной бухгалтерской книги* в том, чтобы устранить необходимость официальной централизованной версии всех финансовых транзакций (на самом деле это в равной степени относится к любой другой области, но пока что давайте ограничимся банками) и заменить ее полностью открытым журналом, копия которого есть у каждого пользователя. Иными словами, вам не нужен банк, потому что эту роль играете *вы сами* и все, у кого есть деньги.

На первый взгляд идея может показаться шокирующей. Каждый пользователь Bitcoin хранит собственную копию журнала со всеми транзакциями, которая отражает реальное состояние финансов в системе. Распределенный журнал в теории выглядит заманчиво, но трудность его практической реализации очевидна. Жизнеспособность этой концепции полностью зависит от того, все ли согласны с содержанием журнала.

Естественно, мы не можем рассчитывать на то, что каждый пользователь Bitcoin будет каждую ночь садиться за стол (с большим бокалом вина) и проверять достоверность каждой транзакции, чтобы установить, куда делся тот или иной биткоин. К счастью, компьютеры лучше справляются с подобного рода задачами. Однако разработка и администрирование согласованной, но в то же время распределенной версии журнала Bitcoin остается непростой задачей. И для ее решения

используется оригинальный подход, почти полностью основанный на криптографии.

Блокчейн Bitcoin

Для реализации распределенного журнала в Bitcoin используется концепция *блокчейна*. Стоит подчеркнуть, что распределенный журнал может и не быть основан на блокчейне, хотя из-за большой популярности системы Bitcoin, в которой одно зависит от другого, эти два понятия зачастую считают синонимами.

Пользователи Bitcoin объединены в одноименную сеть. Каждый из них может иметь столько «счетов», сколько пожелает. У каждого счета есть *адрес* – открытый криптографический ключ, с помощью которого можно проверять достоверность цифровых подписей. Следует отметить, что эти адреса, несмотря на уникальность, не предназначены для явной идентификации их владельца: это обеспечивает анонимность. Транзакция в Bitcoin представляет собой заявление (криптографически подписанное закрытым ключом плательщика) о том, что определенное количество биткоинов должно быть переведено с адреса плательщика на адрес получателя.

Каждый раз, когда в Bitcoin проводится транзакция, сведения о ней становятся доступны всем участникам сети. Таким образом Bitcoin в целом можно считать стопкой свидетельств о транзакциях, которые летают по сети туда-сюда. Учитывая появление новых транзакций раз в несколько секунд, всей этой информацией нужно достаточно четко управлять, чтобы каждый пользователь был согласен с происходящим.

Блок – это набор транзакций в Bitcoin (примерный эквивалент платежей, проведенных за десять минут)[142]. Каждый раз, когда формируется и одобряется новый блок, он «приклеивается» к предыдущим блокам, формируя постоянно растущую *цепочку*. Этот расширяющийся набор блоков, привязанных друг к другу, и составляет журнал Bitcoin. Поскольку все блоки состоят из данных, для их соединения требуется цифровой «клей». Возможно, вы помните, что соединение данных между собой – один из множества способов применения швейцарского ножа от криптографии – хеш-функции.

Если бы все пользователи в сети Bitcoin постоянно формировали новые блоки и пытались одновременно присоединить их к блокчейну, получился бы настоящий хаос. Откуда может взяться единая согласованная версия блокчейна? У этой задачи есть хитрое решение: сделать процесс формирования блоков достаточно сложным, но не невозможным. Как результат, новые блоки создаются медленней, примерно раз в десять минут. Это достаточно быстрый темп для того, чтобы новые транзакции оказывались в журнале без существенной задержки, но достаточно медленный, чтобы новые блоки успевали распространяться по сети Bitcoin, и большинство пользователей имели возможность их одобрить, прежде чем появится следующий блок.

Процесс создания нового блока, лежащий в основе Bitcoin, называется *майнингом* (от англ. mining – добыча полезных ископаемых). Вам не показалось: термин и должен намекать, что это требует существенных усилий. Задача майнинга – собрать ожидающие своей очереди транзакции, которых еще нет в блоках текущего блокчейна, проверить, правильный ли у них формат, и связать их вместе при помощи криптографии. В рамках этого процесса майнер должен прикрепить к началу нового блока некие данные – *заголовок*. Этот заголовок содержит сведения о том, какой блок, по мнению майнера, находится в данный момент в конце блокчейна (к нему должен быть присоединен этот новый блок), и криптографическую «сводку» обо всех транзакциях в новом блоке. Но у заголовка есть еще один элемент, который и делает майнинг новых блоков таким сложным.

Как вы помните, хеш-функции представляют собой криптографические «соковыжималки», которые сжимают входные данные в небольшое число (хеш). Если захешировать какие-то данные, любое изменение в них будет приводить к получению новых хешей без какой-либо видимой связи между ними. Иными словами, хеш выглядит так, будто он сгенерирован случайным образом. Поэтому, если вы хотите подобрать данные с *определенным* хешем, вам остается только хешировать разные значения, пока не повезет.

Именно с этой проблемой сталкивается майнер биткоинов. Он должен включить в заголовок блока случайно сгенерированное число, которое наделяет хеш всего заголовка определенным свойством. Как только майнер собрал достаточное количество транзакций, чтобы

сформировать блок, он приступает к перебору случайных чисел в надежде на то, что одно из них приведет к получению нового блока с правильным хешем. Это несколько суматошный процесс, так как сформировать новый блок пытаются майнеры со всей сети, соперничающие между собой. Тот, кто сделает это первым, «выиграет». Но какова награда?

Никто в здравом уме не стал бы тратить существенные ресурсы на создание новых блоков просто ради забавы. В процессе майнинга приходится перебирать миллионы и миллионы нечетных случайных чисел. Вариантов так много, что успешному майнеру биткоинов необходимы очень серьезные вычислительные мощности[143]. Поэтому тот, кому удается создать новый блок, получает финансовую награду, конечно же, в биткоинах.

Как только новый блок сформирован, об этом уведомляются все пользователи сети Bitcoin, каждый из которых добавляет этот блок в свою локальную версию блокчейна (ту, которую они в настоящий момент считают корректной). Любой пользователь может проверить достоверность этого нового блока и убедиться в том, что его версия блокчейна – та же, что и у всех остальных. Но они могут быть уверены только в *достаточной степени*, поскольку существует вероятность, что два разных пользователя примерно в одно и то же время сгенерировали два разных блока. В таком случае возникают две разные версии блокчейна, на конце которых находятся разные блоки[144].

Эта проблема неизбежная, но разрешимая. После нахождения *следующего* блока одна из этих версий блокчейна расширяется дальше. Всякий раз, когда пользователь Bitcoin сталкивается с разными возможными версиями блокчейна, он выбирает ту, которая длиннее. На практике большинство транзакций в течение получаса с момента их проведения почти наверняка оказываются в общепринятой версии блокчейна (любые отличия могут найтись только в самом конце блокчейна, и их урегулирование происходит довольно быстро).

Блокчейн то, блокчейн се

Bitcoin – это волшебный криптографический механизм. Счет привязан к криптографическому ключу, транзакции являются заявлениями с цифровыми подписями, формирование новых блоков требует решения криптографической задачи, а сам блокчейн собран воедино с помощью хеш-функций. Вот почему Bitcoin наряду с сотнями аналогичных систем цифровых денег, существующих сегодня, часто называют *криптовалютой*[145]. Но причина, по которой мы обсуждаем здесь эту технологию, заключается в том, что блокчейн Bitcoin представляет собой в первую очередь механизм безопасности для обеспечения целостности данных, в данном случае целостности транзакций.

Блокчейн Bitcoin не лишен недостатков. Например, то, сколько вычислительных ресурсов и энергии уходит на формирование новых блоков, вызывает серьезные опасения относительно экологической устойчивости Bitcoin. Время от времени затраты на майнинг превышают ценность сгенерированной валюты. Но, как уже отмечалось, для реализации распределенного журнала необязательно использовать блокчейн так, как это делает Bitcoin.

Распределенные журналы не ограничиваются цифровой валютой, область их применения гораздо шире. Их можно (по крайней мере, теоретически) использовать для защиты любых данных, которые не являются конфиденциальными, но требуют абсолютной целостности: прежде всего это любые учетные данные, включая юридические договоры, документацию о цепочках поставок и правительственные реестры.

Как мы уже видели, явное преимущество распределенных журналов состоит в том, что для обеспечения целостности данных они не требуют единого центра доверия. Но это не означает, что в блокчейн или любой другой распределенный журнал нужно переносить все подряд. Архитектура распределенных журналов существенно отличается от традиционного подхода, когда для обеспечения целостности данные помещаются в защищенное централизованное хранилище. Распределенные журналы защищают данные совсем не так, как это обычно делается в настоящий момент. Это потрясающая концепция, но, если не считать Bitcoin, эффективность ее применения в качестве механизма обеспечения целостности данных еще предстоит доказать.

Целостность целостности

Сложно переоценить то, насколько важна целостность данных в нашей повседневной жизни. В материальном мире она зачастую обеспечивается опосредованно. Но в киберпространстве, где информацией относительно легко манипулировать, целенаправленное обеспечение целостности данных превыше всего.

Механизмы, обеспечивающие целостность данных, неспособны защитить их от внесения изменений, но могут предупредить нас об этих изменениях. Выбор механизма зависит от того, что в вашем представлении может пойти не так. Дружественное окружение вроде системы каталогизации книг в публичной библиотеке нуждается самое большее в легковесных средствах. Враждебные среды, начиная с собственно Интернета, требуют строгих механизмов обеспечения целостности, таких как имитовставки и цифровые подписи. Если у вас нет единого места, которому вы могли бы довериться в вопросе целостности данных, можно даже подумать о развертывании распределенного журнала.

Механизмы обеспечения целостности данных на самом деле работают. Поэтому если выбрать действительно подходящий, преступникам, как правило, *не* удается модифицировать сумму вашего банковского перевода, отредактировать электронное письмо от вашего провайдера или удалить предыдущие транзакции в блокчейне Bitcoin. А не удается им это потому, что у них попросту *нет возможности* это сделать, по крайней мере так, чтобы этого никто не заметил.

Однако эти механизмы могут лишь гарантировать, что данные не менялись с момента их создания… владельцем ключа, на котором основана имитовставка или подпись, или обладателем закрытого ключа, связанного с адресом Bitcoin, – кем бы он ни был.

Серьезные киберпреступники не тратят время на попытки манипулировать данными, целостность которых защищена. Куда более эффективная стратегия состоит в том, чтобы выдать себя за кого-то другого. Если вас ввели в заблуждение относительно личности того, с кем вы общаетесь в киберпространстве, целостность любых данных, которые вы получаете, не слишком велика: примерно как польза биткоина, когда вам нужно подбросить монету.

6. Кто там?

Возможность хранения секретов и обнаружения изменений, вносимых в данные, очень важна. Но она никак не помогает бороться, наверное, с важнейшей угрозой в киберпространстве. Каждый день тысячи людей оказываются обманутыми ввиду того, что в киберпространстве крайне легко выдать себя за другого. Криптография сама по себе не защищает от этой проблемы, но может поспособствовать ее решению.

Гав-гав!

Чтобы проиллюстрировать проблему анонимности в Интернете, часто приводят знаменитый рисунок из журнала *New Yorker*, опубликованный в 1993 году[146]. На нем изображены две собаки, одна из которых сидит за компьютером, положив лапы на клавиатуру, и лает, повернувшись к своему товарищу: «В Интернете никто не знает, что ты собака». Отличная иллюстрация. Мысль о том, что собаки могли бы пользоваться Интернетом без нашего ведома, кажется одновременно забавной и странной. Но оглушительный успех этого рисунка вполне объясняется тем, что в своей невинной манере он отражает мрачную реальность.

Несмотря на поразительное умение доставать куски колбасы из-за дивана, собаки лишены навыков владения клавиатурой. Может, нам бы и хотелось пообщаться с ними в Интернете, но мы понимаем, что их там нет. Вопрос в том, кто же там есть?

Рассмотрим такой случай. Хлое двенадцать лет, и она большой фанат социальной сети, в которой можно легко распространять короткие видеоролики, записанные на телефон, например, танцуя под любимую музыку. Там зарегистрированы все ее друзья, и почти каждый день они публикуют что-то новое. К счастью, Хлоя – послушная девочка, а ее родители осознают потенциальную опасность Интернета и научили ее делиться видеороликами только с теми, с кем она дружит в реальности. Хлоя не разрешает просматривать свое

творчество «друзьям друзей», так как родители предупредили, что ее друзья могут быть не настолько осторожными. И все идет хорошо, пока однажды вечером родители не решили проверить учетную запись своей дочери.

«Ты делишься роликами только со своими друзьями?» – интересуются они.

«Да», – отвечает Хлоя.

«Ты действительно дружишь со всеми этими людьми?»

«Да. Ну, почти, – признается Хлоя. – Есть одна собачка, очень забавная. У нее есть своя учетная запись, поэтому я на нее подписана. Видео – улет; хотите посмотреть?»

«Может, чуть позже, – отвечают родители, – но ты правда дружишь с этой собачкой?»

«Ну, – начинает Хлоя с виноватым видом, – я подписалась на собачку, а та спросила, можно ли ей подписаться на меня, и я разрешила. Ну в смысле, это же собачка, и видео у нее очень, очень смешные; вот мое любимое…»

Это горькая правда, стоящая за иллюстрацией в *New Yorker*: в Интернете не все всерьез задумываются о последствиях того, что вы – *не* собака.

Необходимость знать, с кем мы имеем дело

Подумайте о том, чем вы ежедневно занимаетесь в киберпространстве. Во многих случаях вам необходимо сначала ответить на вопросы вида: «*есть ли у вас учетная запись?*» или «*вы зарегистрированы?*». Действительно, на подобные вопросы приходится отвечать даже при первом посещении киберпространства. Задумывались ли вы над тем, для чего это делается?

Например, большая часть нашей деятельности в Интернете имеет отношение к коммерческим услугам. Киберпространство хоть и является нематериальной, абстрактной концепцией, но в его основе лежат оборудование, сети и сервисы, управляемые живыми людьми и требующие финансирования. Коммерческим поставщикам этих компонентов зачастую нужно знать, с кем они имеют дело, чтобы, по крайней мере, отправить счет по нужному адресу.

Даже за бесплатные, на первый взгляд, виртуальные услуги приходится платить, почти всегда – правом доступа к своим личным данным и просмотром коммерческой рекламы. Поставщики этих услуг должны знать, кто ими пользуется, чтобы иметь возможность сопоставлять собираемую информацию и предлагаемую рекламу с профилями своих пользователей[147].

Идентификация людей в киберпространстве необходима еще и потому, что огромный объем цифровой информации предназначен для ограниченной аудитории. Мало какая компания смогла бы нормально работать, если бы все ее работники всегда знали обо всем, что происходит. В секретных правительственных и военных организациях строгий контроль доступа к данным особенно важен. Кстати, я надеюсь, вы не забываете о настройках приватности своих учетных записей в социальных сетях, чтобы контролировать то, кто может видеть публикуемую вами информацию. Прежде чем делиться своими данными в киберпространстве, стоит сначала определить, с кем вы имеете дело.

В киберпространстве нет собак, даже жесткошерстных такс. Но кто-то же там *есть*! Безопасность нашей виртуальной деятельности во многом зависит от того, насколько точно мы себе представляем, кто нас окружает. Проблема в том, что получить достоверную информацию об этом очень сложно. Чаты, соцсети и сайты знакомств были бы намного безопасней, если бы мы могли решить эту досаднейшую проблему.

Человек против компьютера

Процесс *аутентификации сущности* – это и есть попытка определить, с кем мы имеем дело. Абстрактное слово *сущность* выбрано неспроста. Способы аутентификации могут варьироваться (по крайней мере, частично) в зависимости от того, что эта сущность содержит – пульсирующее сердце или микрочип с тактовой частотой.

Рассмотрим один из подходов к аутентификации сущностей в материальном мире. Путешественник подходит к пункту пограничного контроля. Сотрудник иммиграционной службы должен определить,

имеет ли путешественник право въезда в страну. Он просит предъявить паспорт.

Паспорт – это документ с немаленьким набором физических защитных механизмов. Современные паспорта содержат голограммы, специальные чернила, компьютерные чипы и биометрическую информацию о том, кому они выданы, и все они предназначены для того, чтобы затруднить подделку паспорта и привязать его к определенному владельцу[148]. Паспорт – это результат довольно трудоемких административных процессов, направленных на то, чтобы минимизировать вероятность выдачи его не тому человеку. Сотрудник на пункте контроля, скорее всего, пропустит путешественника, если его паспорт окажется действительным и будет принадлежать ему, а не кому-то другому.

Важно, что в ходе пограничного контроля во внимание принимается *сочетание* человека и его паспорта. Если вы бодро сообщите свое имя, не имея при себе документов, или предъявите паспорт, натянув на голову бумажный пакет, вас никуда не пустят.

В киберпространстве аналоги паспортов создаются довольно легко. Вам, несомненно, часто приходится вводить пароли, номера банковских карт и другие маркеры безопасности для доступа к виртуальным услугам. Они почти наверняка были получены в результате какого-то административного процесса, который мог заключаться лишь в предоставлении адреса электронной почты, позволяющего связать вас с определенным сервисом. В киберпространстве предъявить такой маркер относительно легко; намного сложнее продемонстрировать присутствие человека, которому он был выдан. Увы, но в Интернете все носят на голове бумажные пакеты.

Конечно, аутентификация сущностей не всегда настолько важна. Через пограничный контроль проходят живые люди со всеми их недостатками, поэтому важно знать, кого мы пускаем в страну. То, чем мы занимаемся в киберпространстве, за редкими исключениями имеет намного меньшее значение. Веб-продавец был бы в восторге от информации о том, кто пользуется его сайтом: это позволило бы ему делить своих посетителей на группы в зависимости от их действий и выборов. Но он может извлечь выгоду из пользовательских данных и

без точной идентификации каждого, кто открывает страницы его магазина.

Обратите внимание, что ценность сведений о конкретной сущности в киберпространстве не всегда очевидна. Оператор сотовой связи хочет знать, куда отправлять счет. Поэтому сущностью, которую он хочет аутентифицировать, является владелец учетной записи; и это необязательно тот, кто пользуется услугами, как в случае, когда родители покупают телефон ребенку. С другой стороны, владелец сотового телефона хочет, чтобы в случае его потери им не смог пользоваться любой, кто его найдет. Поэтому сущность, которая интересует владельца, – тот, кто пользуется телефоном[149].

Добавляет путаницы и наш собственный взгляд на то, с кем мы имеем дело. Часто возникает впечатление, что люди в киберпространстве общаются напрямую, а компьютеры служат лишь скромными посредниками. Но это в основном иллюзия. На самом деле все, что происходит в киберпространстве, сводится к взаимодействию компьютеров. Идея о том, что на противоположном конце канала в киберпространстве всегда находится человек, небезопасна, поскольку это зачастую не так. Даже если ваш телефон находится у вас в руках, он способен делать всевозможные удивительные вещи без вашего разрешения. Большинство из них не представляют собой никакой опасности и даже могут быть желанными, например проверка обновлений или извлечение сообщений с сервера. Однако если не проявить достаточной бдительности, ваш телефон может оказаться инструментом опустошения вашего банковского счета и перевода средств незнакомцам[150].

Даже если люди непосредственно участвуют в цифровом взаимодействии, проблема возникает как минимум из того факта, что люди и компьютеры – разного рода сущности (по крайней мере, сейчас), и, строго говоря, на любом конце коммуникационного канала находится не человек, а компьютер[151].

Чтобы это продемонстрировать, рассмотрим простейший пример взаимодействия с киберпространством. Вы сидите за своим компьютером и набираете электронное письмо. Для этого вы формулируете свои мысли в слова и затем переносите их в компьютер, нажимая клавиши на клавиатуре. Вы явно присутствуете во время этого процесса и, несомненно, взаимодействуете со своим

компьютером напрямую. Что плохого здесь может случиться? *Вы* же на месте.

Скорее всего, все будет в порядке, но многое *может* пойти наперекосяк. После того как вы нажали клавишу на клавиатуре, управление берет на себя компьютер. Человек (то есть вы) больше не является частью процесса. Запускается целая цепочка невидимых операций, начиная с того, что введенные символы сопоставляются с цифровыми кодами, которые затем передаются в обработку приложению, запущенному на устройстве. Если ваш компьютер работает как следует, все пройдет гладко. Но если он заражен *вредоносным ПО* (нежелательной программой, чаще всего – компьютерным вирусом), может случиться что-то, чего вы не ожидали. Например, ваш компьютер может сохранить то, что вы ввели, и отправить кому-то, кто за вами следит. Или он может скрыть или изменить введенные вами данные, в результате чего адресату будет послано другое электронное письмо[152]. Может быть, вы уже даже сталкивались с чем-то подобным. В этой ситуации ключевую роль играет поведение вашего компьютера.

Тем фактом, что компьютер может действовать не так, как того ожидает пользователь, или выполнять действия, о которых неизвестно человеку, часто пользуются злоумышленники. Этот разрыв между людьми и устройствами непреодолим, поэтому нам нужно как-то его контролировать. Один из подходов, с которым вы точно сталкивались – *капча* (от англ. captcha – «completely automated public Turing test to tell computers and humans apart», что переводится как «полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей»). Капчи используются для проверки присутствия человека; для этого ставится задача, с которой компьютеры, по крайней мере пока, плохо справляются, например определение того, какие буквы изображены на картинке с неразборчивыми каракулями, или на каких фотографиях из представленных есть автобусы или магазины[153].

Любите вы их или ненавидите (я бы поставил на последнее), необходимость в капчах – это признак разрыва между людьми и компьютерами. И этот разрыв как минимум следует учитывать при определении того, с кем мы имеем дело.

«Привет с другой стороны»

Попробуйте прокричать в киберпространстве: «Привет, кто там?» Даже если в ответ раздастся слабое: «Это я», чего может стоить ответ, пришедший из ниоткуда?

Любой исчерпывающий ответ состоит из двух важных элементов, один из которых касается личности, а другой – времени.

Как и в случае с физическими механизмами безопасности, чтобы отличить одну сущность в киберпространстве от другой, ее необходимо снабдить особенностью, которая будет выделять ее на фоне остальной толпы. Это можно сделать множеством разных способов; выбор зависит только от того, является эта сущность человеком или компьютером.

Человеку, присутствие которого нужно проверить, можно передать материальный объект и попросить его продемонстрировать наличие этого объекта. В киберпространстве могут существовать такие вещи, как смарт-карты, токены и даже телефоны, владение которыми свидетельствует о человеческом присутствии. Конечно, самой серьезной проблемой аутентификации сущностей, основанной на владении объектами, является то, что эти объекты могут быть утеряны или похищены.

Люди, впрочем, и сами по себе могут считаться объектами. Область *биометрии*[154] основана на выделении характеристик человека и использовании их для аутентификации сущности. Эффективность биометрии может варьироваться, но некоторые ее реализации хорошо себя зарекомендовали. Авиапассажиры и осужденные преступники знакомы с процедурой снятия отпечатков пальцев и автоматическим распознаванием лиц; обе эти технологии применяются и в киберпространстве. Биометрические характеристики не так просто потерять или похитить, по крайней мере если речь идет о физических особенностях людей, к которым они относятся[155]. Тем не менее это просто результаты измерений, преобразованные в цифровые значения. Если эта информация каким-либо образом скомпрометирована (например, если кто-то похитил базу данных, в которой они хранились), возникают серьезные проблемы. Вас, скорее всего, не раз

просили сменить пароль, но что если кто-то попросит вас сменить отпечатки пальцев?

Самый распространенный метод аутентификации сущностей в киберпространстве, несомненно, основан на знании того, что неизвестно другим. Этот подход можно использовать для аутентификации как человека, так и компьютера. В этом контексте существенное преимущество компьютеров в том, что у них обычно не возникает проблем с запоминанием сложных вещей, таких как устойчивые пароли или криптографические ключи. Большинство способов применения криптографии для аутентификации сущностей основано на использовании секретной информации в качестве отличительной характеристики.

У каждого метода есть сильные и слабые стороны, поэтому в киберпространстве нередко применяется сразу несколько. Классическим примером *двухфакторной* аутентификации сущностей можно назвать предоставление банкомату как банковской карты (материального объекта), так и PIN-кода (секретной информации). Проверяется в этом случае *наличие* банковской карты, так как она содержит чип с криптографическими ключами для защиты транзакции. Однако знание PIN-кода создает дополнительный аутентификационный слой: мы демонстрируем, что человек, которому известен PIN-код, тоже присутствует. Таким образом этот двухфакторный механизм пытается аутентифицировать сразу две разные сущности: карту и ее владельца. К сожалению, при покупке вещей в Интернете банки не проявляют такую бдительность и не требуют использования платежных терминалов[156]. Конечно, большая часть случаев мошенничества совершается именно во время транзакций *без присутствия карты*[157].

Стоит отметить, что аутентификация сущностей не всегда сводится непосредственно к *идентификации* присутствующих сторон. В некоторых ситуациях достаточно установить, что присутствующее лицо является *авторизованным*[158]. Например, сейчас во многих городах проезд в общественном транспорте можно оплатить с помощью предоплаченных смарт-карт. Чтобы разблокировать турникет и позволить пассажиру пройти, сканер железнодорожных билетов должен определить, достаточно ли средств на карте, и только. В *идентификации* пассажира нет необходимости, хотя некоторые

системы могут выполнять и ее по другим причинам, таким как профилирование маршрутов.

Второй элемент ответа на наши крики в киберпространстве касается времени. Если вы прокричите: «Привет, кто там?» – в глубокую темную пропасть и услышите в ответ: «Это я», можно ли считать ответившего живым человеком? Или это записанный голос? Когда похитители обнародуют видеозапись с заложниками, одна из задач, возникающих перед следователями, состоит в определении того, остаются ли жертвы в живых. Поскольку этот вопрос может быть не менее важен и для самих похитителей, в подобных видеозаписях заложников часто заставляют держать в руках свежие газеты в качестве доказательства того, что обращение записывалось после указанной даты[159].

Такое предоставление свидетельств того, что человек жив, может иметь не меньшее значение в киберпространстве. В этом отношении биометрия имеет естественное преимущество перед механизмами вроде паролей. Жертву можно заставить раскрыть пароль и затем бросить ее в колодец, но хорошая биометрическая технология требует, чтобы ответ на вопрос: «Кто там?» – исходил от живого человека.

Однако, как мы уже отмечали, аутентификация сущностей чаще требуется для устройства, чем для человека. Информация может быть записана и *воспроизведена* в киберпространстве позже, поэтому, отвечая на вопрос: «Кто там?» – мы должны доказать, что ответ действительно дается здесь и сейчас. Это называют свидетельством *свежести*, а не присутствием живого человека. Интересно, что криптография позволяет предоставить доказательство свежести, не полагаясь на часовые механизмы.

Таким образом надежные методы аутентификации сущностей должны указывать на свежесть ответа и устанавливать либо личность, либо полномочия (либо и то и другое). Однако самый распространенный механизм такого рода, который вы ежедневно используете в киберпространстве, – ввод пароля – этого не делает. Это лишь одна из многих причин, почему его нельзя назвать хорошим средством аутентификации.

Агония паролей

Кажется, что в киберпространстве невозможно сделать что-либо без ввода пароля. Пароли стали стандартным подтверждением присутствия кого-то конкретного. Когда вы заходите на веб-сайт (а равно в компьютер или приложение), вам обычно приходится вводить имя пользователя и пароль. Пароли пользуются популярностью, поскольку их воспринимают как простое средство аутентификации сущностей. Но это во многом не так, поэтому их столь же часто ненавидят. Элизабет Стоберт в своей статье назвала это явление *агонией паролей*, и мы все инстинктивно понимаем, что она имеет в виду[160].

Реальная причина, почему паролей следует остерегаться, состоит в том, что они представляют собой очень слабый механизм аутентификации сущностей. Вы, наверное, знакомы с некоторыми недостатками паролей, за которые их критикуют, но стоит все же упомянуть два их основных изъяна.

Во-первых, пароль может относительно легко попасть в чужие руки. У злоумышленника немало способов его заполучить. Находясь рядом с вами, он может просто подсмотреть, как вы вводите его в компьютер (для этого даже придумали термин *shoulder surfing* – подглядывание через плечо), или прочитать на записке, которую вы прикрепили к стене в кабинете. Но даже если злоумышленник от вас далеко, у него все равно достаточно вариантов. Как минимум иногда пароли передаются по сети в открытом виде – незашифрованными. Таким образом, чтобы заполучить пароль, достаточно проследить за вашими действиями в киберпространстве.

Злоумышленник может даже попробовать угадать ваш пароль, поскольку мало кто использует удачные пароли. Чаще всего они состоят либо из личной информации, которую легко получить, либо из слегка видоизмененных слов. Ситуация усугубляется тем, что многие технологии поставляются с общеизвестными паролями, установленными по умолчанию, которые пользователи должны при первой же возможности поменять; на практике же многие не знают, как это делается, или просто не хотят заморачиваться.

Во-вторых, паролям свойственно устаревать. Поскольку их неудобно менять, мы обычно используем один и тот же пароль, пока это вообще возможно. Поскольку у паролей нет такого понятия, как свежесть,

любой, кто получит доступ к вашему паролю, сможет наделать в киберпространстве много бед[161].

С точки зрения злоумышленника, один раскрытый пароль может оказаться полезным, но, если их много, это настоящая находка. Одно из мест, где они могут храниться – компьютер того, кто их запрашивает. Например, чтобы оформить покупку, интернет-магазин может попросить вас ввести пароль. Это удобно для продавца, поскольку он может хранить ваши личные данные (в число которых входит помимо прочего платежная информация) и привязать их к вашим посещениям. Это означает, что где-то в компьютерной системе продавца лежит целая куча паролей. Попытки найти базу данных с паролями – довольно перспективное занятие. И иногда эти попытки успешны[162].

К счастью, никакая уважающая себя организация не станет хранить пароли, применяемые для аутентификации ее клиентов, в открытом виде[163]. На самом деле организации требуется лишь подтверждение того, что некто, входящий в систему, знает свой пароль. Криптография позволяет проверить это, не задействуя сами пароли, достаточно встроить в базу данных какое-то средство проверки корректности (целостности) паролей.

Можно использовать для этого хеш-функции. Идея в следующем. Во время создания учетной записи вы предоставляете организации имя пользователя и пароль. Организация хеширует этот пароль и сохраняет хеш в базе данных вместе с вашим именем. При каждом входе в систему вы заново вводите эту информацию, организация снова хеширует пароль и сравнивает результат с хешем, который хранится в базе данных рядом с вашим именем. Если они совпадают, вы подтвердили свою личность.

В этом контексте хеш пароля может играть ту же роль, что и сам пароль. Если введенный пароль неверен, его хеш будет отличаться от того, который находится в базе данных. Также важно, что любой, кто получит доступ к базе данных, не сможет извлечь пароли из хранящихся там хешей. Такой подход гарантирует, что ваш пароль не знает *никто*, кроме вас, даже администраторы системы. С другой стороны, если вы забудете свой пароль, никто не сможет его восстановить, и вы будете вынуждены его сбросить. Захешированные

пароли подобны жизни человека: мы всегда можем начать новый день, но вернуть утерянное время уже не получится.

Месть справочника

Имя пользователя запомнить легко. Пароль – не настолько… В киберпространстве с этой проблемой сталкивается как невинный пользователь, пытающийся войти в систему, так и злоумышленник. За неимением лучших вариантов пароль можно попытаться угадать.

Красота и неотъемлемый недостаток паролей в том, что они должны быть запоминающимися. Тот факт, что у вас должна быть возможность без труда вспомнить свой пароль, накладывает ограничения на его потенциальную сложность. Как уже отмечалось, в *Оксфордском словаре английского языка* содержится меньше 300 000 слов, и даже если допустить остроумные вариации за счет замены букв другими символами, в криптографическом масштабе количество паролей, которые нужно перебрать злоумышленнику, не так уж велико.

Вот как выглядит настоящая атака на пароли. Злоумышленник составляет список потенциальных паролей. Очевидные варианты, такие как *password, test, abc123* и *justinbieber*, можно разместить в начале; дальше могут идти 300 000 слов, а в конце – их близкие родственники вроде *ju5t1n81e8er*. Имея в своем распоряжении лишь догадки, злоумышленник начинает действовать. Если бы у него была база данных с хешами паролей, он мог бы начать с хеширования. В этом случае он находился бы в куда более выгодном положении: для успеха было бы достаточно совпадения хеша одного из возможных паролей в его списке с *одним* из хешей в базе данных. Как только это произойдет, злоумышленник получит имя пользователя и пароль, которые позволят ему войти в систему. Такая атака называется *перебором по словарю*, так как список, который в ней используется, фактически является словарем паролей.

Перебор по словарю невозможно предотвратить. Его можно затруднить, если использовать вместо паролей кодовые фразы. Если вы это делаете, – замечательно. Однако кодовые фразы сложнее запомнить, вводятся они не так быстро, да и вероятность опечатки выше, чем для простых паролей. Чтобы сделать пароли более

сложными, было предложено много остроумных методов[164], но большинство пользователей попросту не следуют никаким рекомендациям, которые усложняют им жизнь, даже если это может положительно сказаться на безопасности.

И все же то, что нельзя предотвратить, можно попробовать усложнить. Это подводит нас к самому неожиданному способу использования криптографии, с которым мы сталкиваемся ежедневно.

Любой проектировщик компьютерных систем согласится, что криптография – это сплошные неудобства (не самое подходящее слово, наверное)[165]. Выполнение криптографических операций требует времени и усилий. Если у системного инженера есть возможность обойтись без использования криптографии, он ее точно не упустит. Он вам скажет, что безопасность – враг производительности, а криптография замедляет работу систем… Постойте! Кажется, у меня есть идея!

Большинство криптографических алгоритмов рассчитаны на как можно более быстрое выполнение. Но, если говорить о защите от перебора по словарю, у криптографического трактора есть неоспоримые преимущества перед «Феррари». Для хеширования паролей вместо обычной хеш-функции можно специально написать медленную, которая будет выполняться на секунду дольше (в то время как обычно эта операция занимает крошечную долю секунды). Такое замедление входа в систему обычный пользователь едва заметит. Но если словарь паролей злоумышленника состоит из 64 миллионов вариантов (словари такого размера можно купить в Интернете), то намеренная задержка хеширования на одну секунду приведет к тому, что для перебора всего словаря понадобится 64 миллиона секунд – примерно два года. Для такой атаки злоумышленник должен быть либо чрезвычайно терпеливым, либо очень целеустремленным.

Криптографические алгоритмы, играющие роль медленных хеш-функций, иногда называют *алгоритмами расширения ключа*. В организациях нередко применяется несколько слоев таких алгоритмов для защиты паролей, что делает жизнь злоумышленника со словарем еще сложнее. Этот подход, конечно, не делает пароли более надежным средством аутентификации сущностей, но все же помогает сдержать одну из самых опасных атак, направленных на взлом паролей.

Слишком много паролей

Здесь нужен пароль, и там нужен пароль. Этот должен быть не короче восьми символов, а другой должен содержать буквы в верхнем и в нижнем регистре, минимум одну цифру и какой-нибудь еще символ. Утомительно, правда? Что еще хуже, согласно классическим инструкциям о безопасности в Интернете, вы должны позаботиться о том, чтобы все ваши пароли были *совершенно разными*.

Действительно, для каждого сайта и приложения, в которых вы аутентифицируетесь, у вас должен быть отдельный пароль, и тому есть веская причина. Представьте, что вы используете один пароль для всего. Каким бы чудесным он ни был, его безопасность зависит от того, насколько хорошо защищена самая уязвимая система, которой вы его доверили. Ваш банк может управлять паролями на отлично, но уверены ли вы, что владельцы сайта небольшого кемпинга, где вы забронировали место в прошлом году, относятся к безопасности так же серьезно?

Все ли *ваши* пароли удачны и уникальны? Уверены? Правда? Если вы действительно верите в непогрешимость своих паролей, это либо самообман, либо вам помогает криптография.

Тем, кто испытывает проблемы с постоянно растущим количеством паролей, лучше всего воспользоваться специальной системой для работы с ними. Такие системы (известные как *менеджеры паролей*) [166] бывают разных видов, в том числе аппаратные и программные, но основная идея у них одна и та же, они помогают решить три основные проблемы с выбором разных паролей для каждого отдельного случая и дальнейшим их запоминанием. Хороший инструмент такого рода позволит вам генерировать устойчивые пароли, хранить их в надежном месте и автоматически «вспоминать», когда они нужны.

Компьютеру намного легче генерировать и вспоминать устойчивые пароли, чем человеку, поскольку его восприятие ничем не искажено, а память почти безупречна. Менеджер паролей надежно хранит все, что он сгенерировал, в локальной базе данных, зашифрованной с помощью ключа. Пока что звучит неплохо.

Остается решить две проблемы. Первая: каждый раз, когда вас просят ввести пароль, вам нужен ключ для расшифровки базы данных.

Где этот ключ? Вторая: все эти пароли нужны, чтобы аутентифицировать вас, живого пользователя. Менеджер паролей – это программа, запущенная на вашем компьютере (возможно, дополненная аппаратным компонентом). Каким образом все эти хранимые пароли привязаны к вам?

Разные менеджеры паролей отвечают на эти вопросы по-разному, но, наверное, самым распространенным решением в обоих случаях является использование пароля, а чего же еще? Чтобы активировать свой менеджер, вы вводите пароль, из которого затем вычисляется ключ к базе данных. Пароль защищает пароли; чего мы на самом деле этим добились?

В какой-то мере это все-таки шаг вперед. Вместо множества паролей мы теперь имеем дело только с одним. Это намного проще. Да, этот пароль должен быть устойчивым. И да, вы должны его как-то запомнить. И он, конечно же, должен храниться в тайне. Но это всего *один* пароль.

Но это и единая точка отказа. Если ваш менеджер паролей скомпрометирован, вы теряете все сразу. В связи с этим некоторые менеджеры включают более строгие средства аутентификации, чтобы привязать вас к вашим паролям, в том числе биометрию и двухфакторную аутентификацию. Каким бы ни был принцип их работы, все сводится к тому, что они используют шифрование для упрощения работы с паролями, но фундаментальные проблемы паролей остаются. Это борьба с симптомами, а не с причиной[167].

Сплошной маскарад

Нравится нам это или нет, в обозримом будущем пароли так и будут использоваться для аутентификации сущностей. Они глубоко укоренились в роли механизма безопасности, хотя ввиду своей слабости часто провоцируют возникновение уязвимостей, которыми пользуются многочисленные кибермошенники[168].

Вспомните: ранее я упоминал о нескольких разных способах, с помощью которых злоумышленник может заполучить ваш пароль (если предположить, что вы не используете самый передовой

менеджер паролей). Есть еще один, наверное, самый прямолинейный метод: злоумышленник может просто спросить вас.

Успех этой стратегии может казаться маловероятным, но именно так работает *фишинг*. Это атаки, которые проводятся под видом официальных – на первый взгляд – электронных писем, похожих на те, которые вам присылает ваш банк или системный администратор; в них вас просят сделать что-то в целях безопасности, например сбросить ваш пароль. В большинстве случаев жертва щелкает по ссылке, ведущей на поддельный сайт, где у вас первым делом спросят ваш текущий пароль (распространенное требование для сброса пароля). Если вы его введете, можете с ним распрощаться, а возможно, и с номером вашей кредитной карты или той важной секретной информацией, за которой охотились преступники[169].

Потеря пароля может стать началом бесконечных проблем, поскольку с точки зрения любого сайта или приложения, которые используют его для аутентификации, *вы – это ваш пароль*. Все, что с ним делали вы, сможет сделать и мошенник.

Все еще хуже, если фишинговая атака направлена на пароль к вашему менеджеру паролей. Нам бы хотелось верить в то, что смекалистый человек, который использует менеджер паролей, не поддался бы на такую уловку. Но представьте, что вы получили электронное письмо якобы от компании, которая продала вам этот инструмент, и в нем вас просят ввести пароль, чтобы его активировать или обновить (такого у вас не попросит ни одна уважаемая компания). Вы бы его не ввели, правда? Если бы вы допустили такую катастрофическую ошибку, тот, кто стоит за этой атакой, смог бы делать в киберпространстве *все*, что делаете вы.

Стоит бегло проанализировать то, как происходит подобного рода мошенничество. Злоумышленник надевает виртуальный маскарадный костюм, притворяясь вашим банком, чтобы затем выдать себя за вас. Главная проблема состоит в вашей неспособности определить источник исходного поддельного письма и/или сайта, куда оно вас направит. Возможно, вас ввели в заблуждение (слабые) механизмы обеспечения целостности данных, которые придали письму налет официальности (логотипы, деловой стиль, правдоподобие просьбы и т. д.). Но дело в том, что в криптографическом смысле одной лишь видимости целостности данных недостаточно для обеспечения

надежной аутентификации сущностей. Поскольку вы не спросили: «Кто там?» – во время самой фишинговой атаки, в следующий раз, когда один из посещаемых вами сайтов задаст аналогичный вопрос, ответом можете быть вы, даже если это кто-то другой.

В 1990-х один мой друг решил открыть счет в американском банке, и его спросили, какой пароль он себе хочет. К удивлению моего друга, банковский служащий записал ответ в блокнот. На самом деле так с паролями давно никто не обращается. По крайней мере этого делать не следует! Благодаря криптографии ваши пароли не нужно знать никому, кроме вас, и вводить их необходимо только в случае, если вы совершенно уверены в том, что пользуетесь настоящей услугой.

Идеальные пароли

Я отношусь к паролям довольно скептически, и неспроста. Но давайте подойдем к этому вопросу с противоположной стороны. Если бы мы могли полностью переделать мир, как бы выглядел идеальный пароль?

Идеальный пароль должен быть непредсказуемым, чтобы его было как можно сложнее угадать или подобрать с помощью словаря. Иными словами, он должен быть сгенерирован случайным образом. Идеальный пароль должен использоваться для входа только в одну систему и не повторяться в других приложениях. Приличный менеджер паролей может удовлетворить оба эти требования. Однако идеальный пароль также должен быть бесполезным для злоумышленника, каким бы способом тот его ни заполучил (подглядывая через плечо, используя кейлоггер, сканируя сеть, по которой он передается, и т. д.). Хм-м… как же этого добиться?

Мы определенно можем сделать шаг в этом направлении. Уверен, вас время от времени (возможно, даже слишком часто) просят *сменить* пароль. Это еще один раздражающий аспект работы с паролями. Даже если вы успешно запомните сложный пароль со всеми его необычными символами, доброжелательный специалист по безопасности вскоре посоветует вам его *поменять*. Надоедливая процедура, однако ее регулярное выполнение снижает риск некоторых угроз, таких как перебор по словарю, и потенциально ограничивает

последствия раскрытия пароля (о чем вы можете даже не догадываться)[170]. Сделать этот процесс менее болезненным поможет использование менеджера паролей, но это все равно будет неудобно. К тому же это не сделает ваши пароли идеальными, поскольку пока их снова не заменят злоумышленник и дальше сможет их использовать.

Допустим, злоумышленник узнал пароль. Чтобы он никак не смог воспользоваться этой информацией, необходимо сделать так, чтобы этот пароль перестал быть действительным. Следовательно, идеальный пароль должен применяться для аутентификации только в одной системе и только *один раз*. После каждого использования идеальный пароль следует менять.

К счастью, для получения идеальных паролей можно использовать криптографию. Высока вероятность того, что вы используете идеальный пароль при каждом входе в свой интернет-банк. Посмотрим, как это работает на практике.

Первый важный аспект идеального пароля состоит в том, что он должен генерироваться случайным образом. По-настоящему случайные значения получить непросто, так как для этого обычно требуется какой-то физический процесс вроде подбрасывания монеты или бросания костей. Чтобы сделать этот процесс более практичным, компьютер извлекает настоящую случайную информацию из белого шума, который, к примеру, возникает в результате паразитных колебаний в транзисторах. Но, как уже отмечалось, одно из основополагающих свойств любого хорошего криптографического алгоритма состоит в том, что его вывод должен *выглядеть* случайно сгенерированным. Он никогда не сможет вернуть по-настоящему случайное значение, так как его вывод в определенном смысле предсказуем. Если зашифровать один и тот же текст, используя те же ключ и алгоритм, результат всегда будет неизменным. Точно так же, если хешировать одни и те же данные с помощью одной и той же хеш-функции, итоговые хеши получатся идентичными. С другой стороны, когда вы подбрасываете монету, результат всегда непредсказуем.

Однако эта предсказуемость криптографических вычислений не будет проблемой, если позаботиться о том, чтобы криптографический алгоритм каждый раз получал новый ввод: тогда и вывод будет каждый раз новым. Таким образом, использование разного ввода при каждом

выполнении алгоритма означает, что его вывод может стать идеальным паролем.

Идея, лежащая в основе использования идеальных паролей для аутентификации в интернет-банке, состоит в том, что банки могут применять разные технологии. Довольно распространенным подходом является выдача клиенту небольшого устройства, *токена*[171]. У некоторых токенов есть экран, другие напоминают карманный калькулятор. Какое бы устройство ни выдал вам банк, это, в сущности, криптографический алгоритм и ключ. Алгоритм один для всех клиентов банка, а ключ уникален и принадлежит только вам. Все ключи, выданные клиентам, хранятся в базе данных банка.

Во время входа в систему ваш токен генерирует идеальный пароль, используя алгоритм и ключ, и выводит его на экран. После того как вы ввели этот пароль, банк проводит те же вычисления, используя свою копию ключа. Если результат совпадет с вашим, банк может быть уверен в том, что он имеет дело с вами. Если быть более точным, банк уверен, что тот, кто к нему обращается, имеет доступ к криптографическому ключу, который вам выдали. Если кто-то похитит ваш токен, может возникнуть проблема, поэтому во многих банках предусмотрен еще один слой аутентификации (например, некоторые токены сами спрашивают: «Кто там?» – требуя ввести PIN-код).

Токен генерирует пароли криптографическим путем, что делает их в достаточной степени случайными. Для этого обычно применяется специально разработанный алгоритм, но, в принципе, точно так же можно было бы использовать обычные алгоритмы шифрования или имитовставок. Важнее всего то, что ввод, который передается алгоритму, используется для вычисления только одного пароля. В следующий раз, когда банк попросит вас аутентифицироваться, ввод алгоритма должен быть другим. Таким образом при каждом входе в интернет-банк вы будете вводить новый пароль.

Стоит отметить, что ввод алгоритма в вашем токене необязательно хранить в тайне. Единственный секретный элемент этой системы – ключ, который вам выдает банк. Ввод должен быть известен и вам, и банку, и он должен меняться каждый раз, когда банк интересуется тем, с кем он имеет дело. Что же это может быть?

Многие токены содержат часы и подают на вход криптографическому алгоритму текущее время. Этот подход

применяется в токенах, у которых нет клавиатуры; идеальный пароль обычно вычисляется раз в 30 секунд или около того и отображается на экране. Клиент отсылает банку текущий пароль как доказательство того, что прямо сейчас ключ (токен) находится в его владении. Конечно, часы со временем сбиваются, но банк может отслеживать и компенсировать отклонение отдельного токена[172].

Время – это лишь один пример несекретных данных, которые могут быть известны одновременно двум сущностям в разных уголках киберпространства. Если часы использовать нельзя, можно прибегнуть к концепции искусственного времени, имеющей вид счетчика. В этом случае банк и токен используют счетчик для отслеживания того, сколько раз они участвовали в процессе аутентификации. Последний показатель становится несекретным вводом для алгоритма. При каждой попытке входа банк и токен наращивают счетчик и получают новое общее значение.

Таким же образом работают многие автомобильные дистанционные системы. Машина и брелок снабжены одними и теми же криптографическим алгоритмом и ключом, и счетчик у них тоже есть. Каждый раз, когда вы нажимаете кнопку, чтобы открыть машину, брелок вычисляет и передает идеальный пароль. Машина проверяет его корректность и, если все хорошо, открывает замок[173].

Но есть и другой способ получения идеальных паролей, не требующий использования синхронных часов или счетчиков. Гибкость, которую дает отсутствие необходимости в синхронизации, стала причиной того, что этот альтернативный подход лежит в основе не только токенов с идеальными паролями, но и аутентификации сущностей, которая применяется для доступа к Wi-Fi, посещения защищенных веб-сайтов и многого другого.

Цифровые бумеранги

Охотник одного из туземных племен неслышно подкрадывается к краю прибрежного болота в восточной Австралии. Вдалеке плещутся ничего не подозревающие утки. Охотник размахивается и бросает свой бумеранг. Тот огибает дальний берег болота и возвращается назад, летя

низко над водой. Пока утки взлетают, бумеранг снова оказывается в руке охотника[174]. Вам может показаться, что эта сцена не имеет никакого отношения к теме нашего разговора, но киберпространство наполнено свистом цифровых бумерангов. И без них мы не смогли бы надежно делать и половины того, чем мы там занимаемся.

Чтобы понять, почему, вернемся к нашему охотнику. Допустим, он слепой (что делает метание бумеранга еще опасней). Также предположим, что вместо охоты за добычей он использует бумеранг для изучения окружающей среды. Именно с этой целью мы метаем цифровые бумеранги в киберпространстве.

Хоть наш охотник и не в состоянии наблюдать за полетом бумеранга, в одном он может быть уверен: к нему прилетает тот самый бумеранг, который он метнул ранее (разве что один из его друзей решит организовать замысловатый розыгрыш). Если же вы отправите в киберпространство какие-то данные, и позже они к вам вернутся, вам будет не так просто определить, оригинальные ли они. Вам, к примеру, может прийти копия идентичных данных, которые вы отправляли ранее. В связи с этим мы обычно бросаем в киберпространство только свежесгенерированные случайные числа. Поскольку эти числа новые и выбраны случайным образом, вероятность того, что их копия уже когда-то отправлялась в киберпространство, крайне низка. Поэтому мы, как и охотник, уверены в том, что полученные нами случайные числа действительно именно те, которые мы недавно посылали.

Вопреки своей слепоте, охотнику, возможно, удастся сделать определенные выводы о своем окружении по возвращении бумеранга. Допустим, противоположный берег болота зарос чайными деревьями[175]. Пролетая непосредственно над ними, бумеранг может подхватить их аромат, и слепой охотник, возможно, сумеет сделать выводы о том, где побывал бумеранг, по его запаху. Необходимо подчеркнуть один ключевой момент: это наблюдение стало возможным благодаря тому, что вернувшийся бумеранг отличается от того, который охотник метнул (в данном случае совсем немного).

В киберпространстве мы так же слепы, как и наш охотник. Отправляя случайные числа и получая их обратно, мы не имеем ни малейшего представления о том, где они побывали. Однако у данных есть одно преимущество перед бумерангом – та простота, с которой их можно изменить. Если случайные числа можно модифицировать

способом, позволяющим определить, кто их изменил, с помощью этой информации можно узнать, где именно побывали только что пришедшие данные. Иными словами, цифровые бумеранги позволяют нам получить сведения о том, с кем мы имеем дело[176].

Этот принцип, известный как *вызов-ответ*, можно легко реализовать с помощью криптографии. Вернемся к нашим токенам для интернет-банка. Если у токена есть клавиатура, мы можем использовать механизм вызова-ответа вместо системных часов. В этом случае банк генерирует новое случайное число и отправляет его клиенту. Это *вызов*. Его можно сформулировать так: «Покажи мне, что ты можешь сделать с этим случайным числом». Клиент вводит этот вызов в свой токен, который затем с помощью ключа и криптографического алгоритма вычисляет *ответ* и выводит его на своем экране. Клиент возвращает ответ банку, который провел те же вычисления с использованием того же алгоритма и своей копии клиентского ключа. Банк швыряет в киберпространство случайное число и получает обратно его измененную версию, преобразованную так, как это мог сделать только клиент. Цифровой бумеранг возвращается, и, что важно, банк знает, где он побывал.

Важность вызова-ответа

Принцип вызова-ответа играет ключевую роль в безопасности киберпространства. Большинство реальных процессов, в которых используется криптография, занимаются метанием какого-то рода цифровых бумерангов.

До сих пор я говорил о криптографии как о наборе инструментов, которые обеспечивают такие свойства, как конфиденциальность, целостность данных и аутентификация сущностей. На практике же в большинстве процессов с использованием криптографии участвует сразу несколько сторон и инструментов. Хорошим примером можно считать механизм вызов-ответ: банк генерирует вызов (почти наверняка с помощью криптографического генератора случайных чисел) и отправляет его пользователю, который вводит этот вызов в токен; затем токен применяет к введенным данным криптографический алгоритм, чтобы вычислить ответ и вернуть его

банку; банк вычисляет ответ локально и проверяет, совпадает ли он с тем, что сгенерировал токен.

Криптография в основном применяется в непрерывном потоке запросов: отправь то, сделай се, зашифруй это, отправь снова, и т. д. Все вместе это обычно называется криптографическим *протоколом*. Такой протокол в точности описывает процедуру, которой все должны следовать, чтобы используемые криптографические инструменты смогли обеспечить нужный уровень безопасности. Криптографический протокол – это алгоритм, операции которого выполняются разными сущностями.

Вызов-ответ применяется во многих криптографических протоколах, которыми вы регулярно пользуетесь. Например, когда вы подключаетесь к удаленному сайту через браузер, чтобы обработать конфиденциальную информацию (делаете покупки в Интернете, открываете страницу с электронной почтой, пользуетесь услугами интернет-банка), браузер и сервер (компьютер, на котором размещена страница) общаются по криптографическому протоколу, известному как *TLS* (Transport Layer Security – протокол защиты транспортного уровня)[177]. На одном из первых этапов этого процесса ваш браузер и сайт шлют друг другу случайное число.

Какой бы сложной ни была остальная часть криптографических протоколов, большинство из них начинаются с отправки случайно сгенерированного вызова для получения ответа, потому что определение участников взаимодействия – основополагающая часть любого процесса, связанного с безопасностью в киберпространстве. Протокол TLS согласовывает криптографический алгоритм и устанавливает, какие ключи можно использовать для шифрования и защиты целостности последующего взаимодействия между браузером и сайтом. Какой смысл переходить к общению, если вы не уверены в подлинности сайта, к которому пытаетесь безопасно подключиться?

Протокол безопасности, применяемый в Wi-Fi, аналогичным образом определяет ключи для защиты данных, которыми устройство обменивается с сетью, но зачем начинать взаимодействие, если устройству закрыт доступ к беспроводной сети, или если сеть не является подлинной? Большинство криптографических протоколов начинают с аутентификации сущности, а большинство механизмов аутентификации начинаются с какой-то разновидности вызова-ответа.

Господин Никто

Тук-тук. Кто там? *Господин!* Какой господин? *Господин Никто!* Как это часто бывает, в любой шутке где-то глубоко запрятана правда. Иногда на вопрос: «Кто там?» – хочется ответить: «Не скажу! Не твое дело!»

Противоположностью аутентификации сущностей является *анонимность*. Люди могут предпочитать оставаться в киберпространстве анонимными по многим причинам. Нам свойственно обращать внимание на отрицательную мотивацию анонимности, включая незаконную деятельность и шпионаж. Но во многих случаях анонимность имеет конструктивные причины. Граждане деспотических режимов, критикующие свое правительство, чаще всего против раскрытия своей личности. Анонимность нередко нужна журналистам. Если взять более приземленный пример, то пользователь сайта может пожелать остаться неизвестным, чтобы никто не записал его личную информацию или чтобы владелец сайта не мог проанализировать его поведение и подсунуть ему адресную рекламу. Существует даже мнение, что концепция анонимности должна быть одним из неотъемлемых прав человека как часть более универсального и фундаментального права на личную жизнь[178].

Может показаться, что анонимность – обычная форма существования в киберпространстве. В конце концов, все механизмы аутентификации сущностей, которые я уже описывал, мотивированы тем, что в виртуальном мире очень легко выдать себя за кого-то другого. Вы не видите, с кем имеете дело, поэтому, чтобы увидеть, имеет смысл использовать идеальные пароли, не так ли? Но правда в том, что в киберпространстве легко быть *вроде бы анонимным*. С настоящей же анонимностью все сложнее.

Находясь в киберпространстве, вы можете чувствовать себя анонимным. У вас может возникать ощущение, что вы сами, устройство, с которым вы взаимодействуете, и все остальное пребываете в неизведанной пустоте; никого нет рядом, никто вас не видит, никто не знает, что вы там. Когда сайт, продающий билеты, вынуждает вас зарегистрироваться, вы с ехидной усмешкой вводите в качестве имени «Микки Маус» и становитесь мультяшным грызуном.

Похожие ощущения возникают, когда вы садитесь за руль: вы оказываетесь наедине с собой, жестянкой на колесах и автострадой, уходящей за горизонт.

У этого ощущения есть отрицательная сторона. В условиях анонимности многим людям недостает сдержанности, и они меньше обычного склонны к соблюдению норм поведения. Похоже, что анонимность раскрывает некоторые не слишком привлекательные черты характера, которые обычно подавляются[179]. Вы могли сталкиваться с чем-то похожим на дороге: некоторая степень анонимности провоцирует конфликты с другими водителями, хотя даже на очень оживленной улице в окружении других пешеходов ничего подобного не случается. В ситуации, в которой прохожий бы извинился, водитель просигналит. А в экстремальных случаях водители ведут себя еще резче.

В киберпространстве кажущаяся анонимность выпускает наружу невиданные страсти. Использование Интернета для повседневного общения позволило укорениться и разрастись множеству социальных недугов. Нападки в виде едких комментариев (*троллинг*), кибертравля и киберпреследование встречаются все чаще, отчасти провоцируемые кажущейся анонимностью[180]. Иногда этим занимаются люди, знакомые с жертвами, но ощущающие безнаказанность. Но самое худшее поведение зачастую демонстрируют те, кто сознательно пытается сохранить анонимность. Достаточно почитать невероятные комментарии под статьями на сайтах газет и магазинов. Некоторые из них вызывают глубокую обеспокоенность, а самые худшие обычно подписаны псевдонимами.

Водитель, демонстрирующий агрессивное поведение на дороге (например, не соблюдающий дистанцию или увлекшийся опасными маневрами), вполне может думать, что его кажущаяся анонимность защитит его от последствий, но это не всегда так. У машин, в конце концов, есть номера, которые можно сообщить полиции и отследить, а на дорогах установлены камеры наблюдения, которые могут помочь в расследовании. То же самое относится и к киберпространству.

Конечно, с точки зрения анонимности киберпространство намного хуже. Каждое устройство с доступом к Интернету имеет уникальный адрес, который служит идентификатором соединения, а иногда и самого устройства. Компании, предоставляющие инфраструктуру,

такие как сотовые операторы и интернет-провайдеры, почти всегда записывают сетевую активность. У вычислительного оборудования обычно есть ряд свойств, как аппаратных, так и программных, по которым их можно идентифицировать. Почти любое действие, производимое в киберпространстве, оставляет следы, и во многих случаях это можно использовать, чтобы свести на нет не очень усердные попытки сохранить анонимность[181].

Если вы действительно хотите оставаться анонимным в киберпространстве, вам придется приложить определенные усилия. Все-таки криптография предоставляет одни из самых действенных механизмов как для идентификации, так и для достижения анонимности.

Чистим лук

Самой известной технологией для сохранения анонимности в киберпространстве является *Tor*. Этот инструмент не дает абсолютной гарантии (что бы это ни значило), но поддерживает анонимность на уровне, достаточном для того, чтобы эту технологию предпочитали не только политические диссиденты и торговцы на черном рынке, но и обычные пользователи, которым нужна конфиденциальность[182].

Tor состоит из специального браузера и сети выделенных *маршрутизаторов*, которые фактически выступают центрами доставки. Маршрутизаторы – это стандартные элементы Интернета. Обычный трафик (без использования Tor) содержит уникальные сетевые адреса как отправителя данных, так и предполагаемого получателя, а сами данные путешествуют из исходной точки в конечную, перемещаясь от одного маршрутизатора к другому, пока не достигнут пункта назначения. Информация об адресах не является секретом, поэтому все промежуточные маршрутизаторы могут видеть, кто, откуда и куда отправляет данные. В этом, собственно, весь смысл: без этой информации они бы не знали, куда дальше направлять трафик.

Трудность обеспечения анонимности состоит в том, чтобы дать маршрутизаторам достаточно сведений для дальнейшей передачи

данных в нужном направлении, не раскрывая при этом, кто, что и кому отправляет. Это похоже на задачу, которую можно было бы решить с помощью шифрования, но если вы просто зашифруете сведения о маршрутизации, никто не будет знать, куда направлять данные. Tor воплощает решение одновременно простое и остроумное.

Обратимся к аналогии. Представьте, что вы хотите разоблачить организацию, в которой работаете, послав некий документ журналисту. Это нужно сделать срочно и анонимно. Проще всего было бы положить документ в конверт с адресом журналиста и вызвать курьера, но курьер мог бы раскрыть вашу личность, зная адреса отправителя и получателя. Чтобы решить эту проблему, в Tor есть сеть «конспиративных квартир».

Для доставки документа с помощью Tor нужно сначала выбрать три случайных конспиративных квартиры в этой сети. Вы помещаете документ в конверт с адресом журналиста. Затем кладете этот конверт в другой – с адресом третьей квартиры, а его, в свою очередь, – еще в один конверт, с адресом второй. Все это помещается в последний конверт, на котором написан адрес теперь уже первой квартиры. Только после этого вы вызываете курьера, и он доставляет этот в меру упитанный пакет на первую конспиративную квартиру. Там первый конверт распечатывается, обнаруживается адрес второй квартиры, вызывается новый курьер и доставляет пакет дальше. Тот же процесс происходит на второй и третьей конспиративных квартирах. В итоге раскрывается конечный адрес, и последний курьер доставляет последний конверт журналисту.

Этот метод может показаться переусложненным, но он действительно эффективен. Полная информация о том, кто отправил письмо и кто его должен получить, неизвестна ни людям на конспиративных квартирах, ни курьерам. Первый курьер и те, кто принял пакет по первому адресу, знают, откуда он прибыл, а третий курьер и люди в третьей квартире знают, куда она направляется, но и то и другое сразу неизвестно никому. В Tor роль конспиративных квартир играют маршрутизаторы, а роль конвертов – уровни шифрования. Данные, отправляемые через Tor, шифруются три раза, и, прежде чем передавать их дальше, каждый маршрутизатор убирает один слой шифрования. Этот процесс иногда называют *луковой*

маршрутизацией, поскольку он похож на то, как повар чистит лук слой за слоем.

Анонимность – ужасно увлекательный аспект киберпространства. Этому множество причин, включая те, которые мы уже обсудили. Однако немало и совершенно противоположных взглядов. Из-за ее отрицательных свойств[183] анонимность считают одной из величайших бед киберпространства. Но для части пользователей она – одна из характерных особенностей свободы в Интернете[184]. Поскольку лучшим средством обеспечения анонимности в киберпространстве является криптография, ее тоже часто как демонизируют, так и превозносят. Но и об этом мы подробно поговорим чуть позже.

Кто есть кто?

Мой анализ того, с кем мы имеем дело, был немного упрощенным. Я рассказывал о разделении между человеком и компьютером, но в реальности все еще сложнее.

Что собой представляет человек в киберпространстве? Большинство людей создают себе разных виртуальных персонажей. Вы как человек известны под разными псевдонимами и публикуете информацию с помощью разных учетных записей в целом ряде сервисов. У некоторых людей даже есть по несколько учетных записей в одном и том же сервисе. Что из этого можно назвать вашей «настоящей» личностью? Все? Что-то одно?

Кто еще, помимо людей, может находиться в киберпространстве? Ноутбук, телефон, токен, ключ, сетевой адрес. Или, может быть, сервер, сетевой маршрутизатор, компьютерная программа… Возможности практически безграничны.

Через десяток-другой лет все будет запутано еще сильнее. Подавляющее большинство людей держат мобильные телефоны при себе, что делает их подходящими устройствами для выполнения аутентификации. Современные мобильные телефоны даже способны надежно хранить ключи и вычислять сложные криптографические алгоритмы. Таким образом, люди все чаще носят при себе настоящие

компьютеры и в будущем рискуют *стать* с ними единым целым. Благодаря достижениям в области диагностики состояния здоровья вполне вероятно, что когда-нибудь мы начнем вживлять себе миниатюрные вычислительные сенсоры. Это может прозвучать угрожающе, но нравится вам это или нет, уже сейчас существуют проекты, исследующие возможность подключения человеческого мозга к киберпространству[185]. А тем временем и сами компьютеры все больше походят на людей. Они начинают осваивать человеческий образ мышления благодаря прогрессу в сфере искусственного интеллекта, а обработка огромных наборов данных позволяет им имитировать решения, принимаемые человеком, и даже предлагать лучшие альтернативы. Достижения робототехники приближают будущее, в котором киборги (в том или ином виде) могут стать реальностью.

К каким последствиям это приведет для аутентификации сущностей, можно только гадать. Но какие бы технологии ни появились в киберпространстве, основной вопрос останется неизменным: «Кто там?» Тот, кто его задает, должен хорошо подумать, кто этот «кто». О ком вам *нужно* знать? О человеке, токене, учетной записи, ключе? Кто именно даст вам ответ? И, с другой стороны, когда аналогичный вопрос задают вам, кто отвечает от вашего имени? Вы или ваш телефон? Это полезно знать, чтобы понимать, какую частицу своей «киберличности» вы теряете, меняя телефон.

Кто там? Ответ на этот вопрос может быть непростым, но для безопасной работы в киберпространстве мы обязаны его знать.

7. Взлом криптосистем

Пришло время проверить наши знания на практике. Криптография предоставляет всевозможные полезные инструменты: механизмы шифрования управляют доступом к информации, механизмы обеспечения целостности определяют, была ли информация модифицирована, а механизмы аутентификации сущностей позволяют узнать, с кем мы имеем дело. Все эти средства выглядят в теории просто прекрасно, но, если мы хотим чувствовать себя в безопасности, возможности, которые они предоставляют, должны быть эффективными в реальных системах.

Разработка реальных систем – процесс крайне сложный, поэтому нам стоит поговорить о том, как криптографию можно превратить из занимательной идеи в то, что действительно будет защищать нас в киберпространстве. А чтобы понять, как криптография должна быть реализована на практике, лучше всего подумать о том, что может пойти не так.

Фундамента недостаточно

Криптография работает. По крайней мере в теории. Тем не менее мы постоянно слышим о том, что ее кто-то «взломал». Письма Марии Стюарт и Наполеона в конце концов были раскрыты, несмотря на использование криптографии. Союзникам удалось расшифровать большую часть переговоров, защищенных с помощью немецких машин Энигма, что дало им огромное преимущество к концу Второй мировой войны. Криптография, применяемая в новых технологиях, часто обнаруживает слабые места. А экспертам-криминалистам иногда удается обходить средства шифрования на изъятых мобильных телефонах. Почему же криптография продолжает подводить?

Разработка хорошего криптографического алгоритма – очень сложная задача, поэтому может возникнуть соблазн свалить все провалы криптографической защиты на слабые стороны самой криптографии. Но на деле такие случаи возникают крайне редко.

Стоит разобраться в том, какую именно роль криптография играет в защите информации как в киберпространстве, так и вне его. Криптография предоставляет ряд механизмов безопасности, каждый из которых имеет строго определенное назначение. Например, шифрование делает данные непонятными. На первый взгляд, это могло бы пригодиться при обеспечении конфиденциальности, но есть один очень важный нюанс, о котором должен знать любой, кто полагается на шифрование, но который можно на свой страх и риск проигнорировать. *Все*, что делает шифрование, – это перемешивает данные.

Чего же оно *не* делает?

Шифрование не дает гарантию того, что его алгоритм был как следует реализован или интегрирован в технологию, которую он должен защищать. Шифрование не следит за тем, кто имеет доступ к ключу для расшифровки. И, наконец, шифрование никоим образом не участвует в защите данных до того, как они были зашифрованы, и после того, как их расшифровали.

Чтобы как следует понять, какую защиту обеспечивает криптография, необходимо принять во внимание тот факт, что ее можно использовать только в рамках *криптосистемы*. Сюда входят, конечно, не только алгоритмы и ключи, но также технологии, на основе которых реализована криптография, устройства и процессы для управления криптографическими ключами, общие процедуры для работы с защищенными данными и даже люди, которые со всем этим взаимодействуют. Когда криптография подводит, это означает, что со своими обязанностями не справилась какая-то часть криптосистемы. Не следует исключать слабые места самих криптографических методик, но проблемы, скорее всего, стоит искать в другом месте.

Криптография жизненно необходима для большинства современных технологий безопасности, применяемых в киберпространстве. Это, если хотите, фундамент, на котором можно построить безопасную систему. Если мы строим небоскреб, без фундамента не обойтись, но только его недостаточно. И если небоскреб, упаси боже, обрушится, причина, скорее всего, не в фундаменте[186].

Использование передовых технологий

Цезарь, судя по всему, был заядлым любителем криптографии. Принято считать, что он применял ее в любых ситуациях, когда его заботила конфиденциальность написанного[187]. Алгоритм, который он применял, вошел в историю как *шифр Цезаря* и заключался в сдвиге букв алфавита. Величина сдвига была ключом, и, как утверждают, Цезарь обычно сдвигал буквы на три позиции (превращая A в D, B в E, и т. д.).

Шифр Цезаря – это, как правило, первый алгоритм шифрования, с которым знакомятся студенты, изучающие криптографию. Он используется в качестве наглядного примера, а затем студенты узнают, насколько он слабый. Шифр Цезаря слишком прост, он выдает информацию об исходном тексте, у него всего двадцать шесть возможных ключей, а сам ключ раскрывается, как только становится известным хотя бы один фрагмент исходных данных, которые соответствуют зашифрованным. Банковские счета так *не* шифруют.

Насколько же наивен был Цезарь?

Юлия Цезаря можно называть как угодно, только не наивным. Хитрый политик, дерзкий военачальник и в конечном счете авторитарный глава Римской республики – этому человеку было что скрывать. Любое применение криптографии в те далекие времена можно назвать лишь провидческим. Сам этот факт говорил о том, что человек знает цену информации и умеет ее защищать. Не забывайте, что по крайней мере часть врагов Цезаря была неграмотна. А те немногие, кто умел читать, вряд ли слыхали о криптографии. Перехватив текст, закодированный шифром Цезаря, они бы были одурачены. Юлий Цезарь понимал, что он делает. Его простенький шифр был передовым методом шифрования, и он почти наверняка справлялся со своей задачей. Аве Цезарь!

В конце шестнадцатого века Мария Стюарт вместе со своими пособниками по заговору Бабингтона составила собственные алгоритмы шифрования, чтобы сохранить переговоры в тайне (тому, кто планировал свергнуть Елизавету I, конфиденциальность была жизненно необходима)[188]. Но ни она, ни ее соратники не были знакомы с передовыми веяниями в области криптографии, и это их погубило. Если бы она как следует изучила научный труд *La cifra del Sig. Giovan Battista Belaso*, который Джован Баттиста Белласо опубликовал в 1553 году, наш мир, наверное, выглядел бы совсем

иначе. Но вместо этого Мария положилась на ряд алгоритмов, которые были разработаны специально для нее и недалеко ушли от шифра Цезаря. У нее не было ни единого шанса против могущественной секретной службы, находившейся в распоряжении Елизаветы. Королева наняла Томаса Фелиппеса, в своем шестнадцатом веке – фактически криптографа, и, что примечательно, Артура Грегори – специалиста по незаметному распечатыванию писем[189]. Мораль этой истории в том, что для защиты информации зачастую требуется как конфиденциальность, так и целостность данных.

Хорошая новость заключается в том, что в наши дни устойчивые криптографические алгоритмы доступны всем. Начиная с 1970-х годов криптография перестала быть прерогативой правительства и военных и действительно расцвела. Криптографические алгоритмы описываются несколькими важными международными стандартами, включая AES, и, по заверениям широкого сообщества специалистов, действительно безопасны[190].

Было бы логично надеяться на то, что технологии, которые мы ежедневно используем в киберпространстве, применяют эти чудесные передовые криптографические алгоритмы, не так ли? Ну, в большинстве случаев это действительно так, но не во всех. Существует ряд грустных примеров, когда в новые технологии внедрялись самодельные алгоритмы. Это делалось по самым разным причинам, часть их даже можно назвать в какой-то мере уважительными, например, некоторые алгоритмы разрабатывались для оптимизации производительности в определенных окружениях. Но зачастую причина была в банальном невежестве. Почти все современные попытки повторить «подвиг» Марии Стюарт закончились плохо, хотя, по правде говоря, никто хотя бы не поплатился головой[191].

Из этого можно извлечь простой урок. Когда речь заходит о выборе криптографического алгоритма (для конфиденциальности, целостности данных или аутентификации сущностей), отдавайте предпочтение самому передовому. Криптографические алгоритмы – ключевые элементы любой криптосистемы, и выбирать имеет смысл только самые лучшие. Если вы применяете алгоритм, пользующийся всеобщим уважением, и с вашей криптосистемой случилось что-то плохое, причина почти наверняка в чем-то другом.

Известное и неизвестное

Конечно, когда специалисты рекомендуют передовой криптографический алгоритм, это означает, что они его таковым *считают*, исходя из своих знаний криптографии. Никакой алгоритм никогда не гарантирует абсолютную безопасность. При размышлениях о чем-то неопределенном будет нелишним свериться с легендарной иерархией познаваемости бывшего министра обороны США Дональда Рамсфельда[192].

Криптографические алгоритмы в основном разрабатываются с учетом *известных известных* методов безопасности. Мария Стюарт потеряла контроль за своей информацией, поскольку она была недостаточно осведомлена в известных известных методах того времени. Ее алгоритмы шифрования имели одно нежелательное свойство, характерное для шифра простой замены, о котором мы говорили в самом начале: при использовании любого определенного ключа каждая исходная буква всегда превращалась в одну и ту же зашифрованную букву. Поскольку в любом языке разные буквы используются с разной частотой, в зашифрованном тексте одни буквы встречаются чаще других, и тщательный анализ частоты их использования позволяет сделать обоснованное предположение о том, какими были исходные буквы. Этот вид *частотного анализа* в сочетании с методом проб и ошибок дает возможность на удивление легко восстановить весь оригинальный текст. В наши дни головоломки такого рода часто публикуются в журналах и считаются слишком простыми для компьютеров.

Частотный анализ – это лишь один из многих способов атаки, большинство из которых намного сложнее, и разработчики современных криптографических алгоритмов должны о них знать. В эпоху Марии Стюарт изобретение частотного анализа привело к переходу на более сложные алгоритмы шифрования, такие как шифр Виженера в исполнении Джованни Баттисты Белласо, в котором одна и та же исходная буква в разных местах исходного текста шифровалась по-разному.

В случае Марии Стюарт частотный анализ принадлежал к категории неизвестного, которая, наверное, не слишком интересовала

Рамсфельда с его привилегированным доступом к самой могущественной разведывательной службе в мире. Это было *неизвестное известное* – то, о чем она не знала, но могла (и, возможно, должна была) знать. Начиная с середины 1970-х, когда криптография начала использоваться широкой общественностью, угрозы неизвестного известного еще не встречались. До этого криптография применялась в основном правительственными и военными организациями, и уже поэтому была окутана тайной.

Когда в конце 1970-х был впервые опубликован алгоритм DES, никто не сомневался, что разведывательные службы знали о криптографии куда больше, чем все остальные. Из-за этой эксклюзивности возникали опасения (вероятно, даже беспочвенные) о том, что алгоритм DES подвержен атакам, о которых могли догадываться только спецслужбы. Оказалось, что подобного рода неизвестные известные действительно существовали, но, похоже, использовались для усиления шифрования, а не для его ослабления[193]. К моменту появления альтернативного алгоритма, AES (который мы обсуждали в главе 3), отставание публичных знаний о криптографии от секретных заметно сократилось.

Сегодня владение криптографией настолько распространено, что вероятность существования серьезных неизвестных известных в сфере разработки криптографических алгоритмов ниже, чем когда бы то ни было прежде, хотя секретные службы, скорее всего, знают кое-что, о чем даже не задумывалась общественность[194]. Когда в 2013 году Эдвард Сноуден раскрыл многочисленные сведения о тайном использовании криптосистем спецслужбами, мало что указывало на то, что эти службы имели какое-либо превосходство в анализе криптографических алгоритмов.

Рамсфельд признал существование *известного неизвестного* – информации о производстве оружия в Ираке, которой, как он знал, не было у разведки США. Несколько известных неизвестных нависают темными тучами и над криптографией.

Впрочем, криптография имеет одну важную предпосылку: злоумышленник не то чтобы *не может в принципе* получить исходный текст из зашифрованного, найти ключ расшифровки, вычислить простые множители большого числа, подделать имитовставку, подобрать ввод с определенным хешем и многое другое. Эти задачи

выполнимы, но очень *сложны*. И уровень сложности, который мы им приписываем, определяется нашими предположениями о том, какой объем вычислительных ресурсов может потратить на них злоумышленник.

Первая трудность состоит в том, что существование опасных злоумышленников ни для кого не секрет, однако мы не знаем, кто они и насколько мощны их компьютеры; мы можем лишь сделать обоснованное предположение[195]. Вторая, более неприятная проблема связана с тем, что мы знаем о постоянном появлении все более быстрых компьютеров, но не о том, как вырастет их мощность и скорость в будущем. По счастью, существуют наблюдения о том, каким образом увеличивается вычислительная мощь, и на их основании можно делать прогнозы, но это тоже из разряда догадок. Из-за этих двух известных неизвестных криптографические алгоритмы отличаются консервативной архитектурой, в которую заложены предположения о существовании настолько опасных угроз, что они вряд ли когда-либо станут реальностью. Лучше перестраховаться, чем потом жалеть.

Однако реальная опасность, нависающая над криптографией, заключается в квантовых вычислениях. Мы *знаем*, что они не за горами. Мы *знаем*, что они будут иметь последствия разной степени серьезности для современных криптографических алгоритмов. Но мы *не знаем*, когда это произойдет. Мы *не знаем*, насколько эффективной будет эта технология на практике. Одно несомненно: квантовые вычисления повлияют на будущее развитие криптографии, так что мы к ним еще вернемся.

Это, наконец, подводит нас к главному опасению Рамсфельда: *неизвестному неизвестному*. Могут ли криптографические алгоритмы, которые мы сегодня используем, стать бесполезными из-за внезапного прорыва, который скомпрометирует их защиту? Надеюсь, нет, но об этом нельзя говорить с уверенностью. В мире разработки криптографических алгоритмов такие сюрпризы возникают нечасто, но один прецедент все же имеется.

В 2004 году на одной из ведущих конференций по исследованиям в области криптографии Ван Сяоюнь, тогда еще относительно неизвестный китайский исследователь, составил неофициальный документ, описывающий невероятно эффективную атаку на MD5 –

одну из главных хеш-функций, которые тогда находились в употреблении[196]. Непосредственной угрозы всем приложениям, опирающимся на MD5, она не представляла, но ясно демонстрировала тот факт, что этот алгоритм *намного* слабее, чем принято считать. Большинство методик, применяемых для таких атак, эволюционируют постепенно, прорывы редки. Неизвестное, о котором прежде не знали, стало известным и спровоцировало процесс, который в конечном счете привел к выработке совершенно новых подходов к созданию алгоритмов хеширования.

Как спасти мир?

Давайте поговорим о практическом применении криптографии, как это часто показывают по телевизору (например, в фильмах о Джеймсе Бонде).

Два агента спецслужб едут в машине, маневрируя по оживленным городским улицам наперегонки со временем. Водитель паникует и срочно связывается со штабом. Пассажир, занудный на вид компьютерщик, только что вставил в свой ноутбук недавно похищенную флешку. «Что на ней?» – спрашивает водитель. «Она зашифрована», – отвечает компьютерщик. «Можешь взломать код?» – спрашивает водитель. Компьютерщик начинает барабанить по клавиатуре, наблюдая за загадочными символами, пляшущими по экрану, прикусывает губу и медленно выдыхает. «Мне еще никогда не встречался такой способ шифрования; он невероятно сложен. Тот, кто это написал, знал, что делает». – «Но ты можешь его обойти?» – рычит в ответ водитель, пока таймер на экране неумолимо приближается к нулю. Компьютерщик, скривившись, снова начинает стучать пальцами по клавиатуре. Камера фокусируется на ноутбуке, по экрану которого стремительным потоком двигаются неразборчивые данные. Водитель проскакивает на красный свет, обгоняет автобус и едва уходит от лобового столкновения с мотоциклом. Компьютерщик все отстукивает по клавишам, бормоча что-то себе под нос, глаза как блюдца, все лицо выражает увлеченность буйством зашифрованного текста на экране. Водитель решает срезать и внезапно поворачивает направо, обнаруживая, что путь заблокирован мусоровозом. Раздается свист

тормозов, водитель вздыхает в отчаянии. Таймер отсчитывает последние секунды. Компьютерщик, задыхаясь, произносит: «Получилось!» И мир опять спасен.

Либо компьютерщик обладал знаниями о неизвестном неизвестном, либо (выражаясь максимально лаконично) это все бред.

Что же произошло? Специалист-криптограф на пассажирском сиденье сообщил, что алгоритм шифрования ему неизвестен. Что заставило его сделать такой вывод? Данные, зашифрованные любым приличным алгоритмом, должны выглядеть так, словно их сгенерировали случайным образом, поэтому обычно на глаз нельзя определить, какой именно алгоритм использовался для шифрования. Но не станем заострять внимание на этой проблеме. Компьютерщик каким-то образом установил, что ни один из алгоритмов шифрования, с которыми он знаком, в этой ситуации не использовался. Он также заявляет, что тот, кто шифровал данные, знал свое дело, так что мы можем уверенно предположить, что ключ для расшифровки на флешке не хранился (в ином случае шифровальщик был бы явно *неквалифицированным*). Таким образом компьютерщику неизвестен алгоритм, и у него нет ключа. Так откуда же берется расшифрованный текст?

Ответ может быть только один. Компьютерщик каким-то чудом умудрился перепробовать все мыслимые алгоритмы и подобрать все возможные ключи к каждому из них. *Все мыслимые алгоритмы*? Сколько всего их существует? На этом даже не стоит заострять внимание: их число так велико, что эту возможность можно уверенно отмести[197].

Давайте начистоту. Если у вас в руках окажется зашифрованный текст и вы не знаете, с помощью какого алгоритма он был создан, проанализировать его будет почти невозможно (если предположить, что он был сгенерирован хорошим алгоритмом шифрования). Но по всем упомянутым выше причинам сегодня криптография чаще всего применяется в соответствии со стандартами, которые в точности описывают используемый алгоритм. Поэтому вполне логично предположить, что алгоритм *известен*.

Давайте исправим этот эпизод нашего шпионского фильма. «Она зашифрована», – отвечает компьютерщик. «Можешь взломать код?» – спрашивает водитель. Компьютерщик начинает барабанить по

клавиатуре, наблюдая за загадочными символами, пляшущими по экрану, прикусывает губу и медленно выдыхает. «Похоже, они использовали чрезвычайно сильное шифрование. AES, наверное. Тот, кто его написал, знал, что делает». – «Но ты можешь его обойти?» Тик-так, тик-так, тик-так… Машина со свистом останавливается, водитель вздыхает в отчаянии. Таймер отсчитывает последние секунды. Компьютерщик, задыхаясь, произносит: «Получилось!»

Как бы не так.

Длина ключа имеет значение

Можно не сомневаться, что Юлий Цезарь об этом знал. Участники заговора Бабингтона тоже, по всей видимости, это понимали. Даже вы, скорее всего, в этом уверены, если дочитали досюда. Удивительно, но некоторые разработчики новых средств безопасности недооценивают этот факт. А сценаристы шпионских триллеров и вовсе предпочитают его игнорировать.

Длина ключа имеет значение. Иными словами, количество возможных ключей довольно заметно влияет на безопасность криптографического алгоритма. Ключей много не бывает, а вот мало – запросто.

Двадцати шести, к примеру, недостаточно! Цезарю их, может, и хватало, но для защиты звонков по мобильному телефону нужно что-то получше. Мария Стюарт со своей расширенной версией шифра простой замены находилась в гораздо лучшей позиции с точки зрения длины ключа. У ее алгоритмов было намного больше ключей, чем у вышеупомянутого шифра (хотя у него с этим тоже не было проблем). Длина ключа, который использовала Мария Стюарт, была почти приемлемой по нынешним меркам. Поэтому напрашивается очевидный вывод: длина ключа важна, но это не *единственный* важный фактор. Достаточный «запас» возможных ключей не гарантирует, что ваша голова останется на плечах.

Длина ключа имеет значение, поскольку против любого криптографического алгоритма можно провести одну незамысловатую атаку. И эта атака работает вне зависимости от того, насколько хорошо алгоритм перемешивает входные данные, прежде чем выдать

шифротекст, имитовставку или что-то другое. Мы всегда можем провести *полный перебор*[198] всех возможных ключей. Для того чтобы у нас были шансы на успех, должны выполняться всего два условия: мы должны знать, что это за алгоритм, и у нас должна быть возможность определить, нашли мы правильный ключ или нет.

Вернемся к переработанной версии нашего вымышленного фильма и рассмотрим возможность полного перебора ключей в контексте симметричного шифрования. У компьютерщика есть какие-то зашифрованные данные, и он хочет получить из них исходный текст. Он знает (или делает обоснованное предположение) о том, что в качестве алгоритма шифрования использовался AES. Но неизвестен ключ. При отсутствии любой другой информации ему остается только перебрать все возможные ключи один за другим. Предположить ключ, расшифровать, повторить. Снова, и снова, и снова. Если предположить, что исходный текст не был случайным, определить, корректен ли ключ, должно быть довольно просто – экран с непонятным шифром превратится в карту и план предстоящей террористической атаки. Но можно ли найти подходящий ключ вовремя?

Я буду откровенен. Если бы ключ к данным, зашифрованным с помощью AES, был найден простым перебором за несколько минут, компьютерщик был бы невероятным счастливчиком. Сколько на самом деле займет поиск подходящего ключа? В большинстве случаев необязательно пробовать *все* варианты (это было бы *невезением* сравнимых масштабов). В среднем при простом переборе ключ находится на полпути. Если бы речь шла о шифре Цезаря, компьютерщик мог бы с легкостью перебрать все 26 возможных ключей, но правильный вариант, скорее всего, нашелся бы где-то на тринадцатой попытке. Он мог бы даже сделать это вручную, но его ноутбук справился бы с этой задачей мгновенно. А что насчет *настоящего* алгоритма шифрования?

Для чистоты эксперимента заменим ноутбук компьютерщика суперкомпьютером (что в реальности сделать невозможно) мощностью 100 петафлопс (100 000 000 000 000 000 операций в секунду). AES имеет (сколько бы вы думали?) как минимум миллиард миллиардов миллиардов миллиардов (340 ундециллионов для тех, кто любит большие числа) ключей. Примерные расчеты показывают, что полный

перебор AES на этом суперкомпьютере занял бы в среднем 50 миллионов миллиардов лет[199]. Это, к сожалению, не поместится в рамки обычной телепрограммы. Если будущее мира зависит от успешного полного перебора AES, мы обречены.

Длина ключа обычно измеряется в количестве бит. Самый короткий ключ AES, на котором были основаны приведенные выше расчеты, занимает 128 бит.

У длины ключа есть два важных аспекта, которым стоит уделить внимание. Их, наверное, лучше всего проиллюстрировать в контексте DES – алгоритма шифрования, который бы использовался в нашем фильме, если бы его события происходили в конце прошлого века.

Первый аспект заключается в чувствительности длины ключа. В DES ключи имеют размер 56 бит, в два с лишним раза меньше, чем в AES. Но это не означает, что у AES в два раза больше ключей, чем у DES. Увеличение симметричного ключа на один бит удваивает количество возможных ключей, и таким образом ключей у AES в 5 секстиллионов (5000 миллиардов миллиардов) *раз* больше, чем у DES! Только представьте себе на секунду.

Второй аспект связан с тем, как меняются рекомендации касательно длины ключа с течением времени. В конце 1970-х, когда был впервые выпущен стандарт DES, высказывались опасения о том, что его 70 миллионов миллиардов ключей может оказаться недостаточно. Согласно тогдашним оценкам, за 20 миллионов долларов можно было собрать компьютер, способный перебрать все эти ключи менее чем за сутки[200]. Но никто такой компьютер так и не собрал: расчеты заставили предположить, что он все равно бы расплавился раньше, чем завершил свой поиск.

Двумя десятилетиями позже ключ DES был найден менее чем за полгода совместными усилиями компьютеров со всего мира, подключенных к тогда еще молодому Интернету[201]. Такое достижение было бы немыслимым в конце 1970-х. На протяжении двух десятилетий DES оставался передовым алгоритмом шифрования, а вычисление его ключей считалось неосуществимым. Но со временем технологии становятся лучше. Рождение AES стало реакцией на осознание того, что длина ключа в алгоритме DES – его слабое место. Современные суперкомпьютеры, которым нужно 50 миллионов

миллиардов лет для поиска ключа AES, способны подобрать ключ DES за время, которого не хватит даже сварить яйцо вкрутую.

Конечно, никто не утверждает, что стандарт AES сохранит актуальность на протяжении всех следующих 50 миллионов миллиардов лет. Компьютеры продолжают развиваться, и это нужно учитывать при рекомендации длины ключа. Поскольку от полного перебора ключей защититься невозможно, мы должны позаботиться о том, чтобы на практике их вряд ли было реально полностью перебрать в разумные сроки. Длина ключа важна, даже если серьезное отношение к ней может испортить случайный фильм.

Важно не то, что вы делаете, а то, как вы это делаете

Наполеон Бонапарт на своем горьком опыте узнал, почему так важно использовать качественную криптографию[202]. В 1811 году он заказал разработку передового алгоритма шифрования, известного как *Le Grande Chiffre de Paris* (великий парижский шифр). Он должен был быть устойчивым к частотному анализу. Используя такие методики, как замену одних и тех же исходных букв множеством разных символов, маскируя часто встречающиеся сочетания букв, этот слегка неуклюжий, но эффективный алгоритм имел шансы взять верх над специалистами-криптографами британской армии и ее союзников.

Le Grande Chiffre был взломан в течение года. Через двенадцать месяцев войска Наполеона неохотно покинули Пиренейский полуостров после поражения в войне, во время которой все их зашифрованные сообщения тайно читали британцы. Еще через два года Наполеона отправили «*в отпуск*» на остров Святой Елены. Он так никогда и не понял, что использование хорошего криптографического алгоритма не гарантирует безопасность. Не менее важно то, *как* вы его используете[203].

Армия Наполеона применяла сильное шифрование, но делала это небрежно. Самой большой ошибкой было то, что военные регулярно шифровали свои послания не целиком. Обмениваясь такой смесью обычного и шифрованного текста, французы сделали британской разведке подарок. Имея на руках фрагменты исходного текста,

британские аналитики могли сделать обоснованное предположение о том, каким должен быть остальной текст, и сопоставить свои догадки с ранее перехваченными переговорами. Для нахождения полного ключа Le Grande Chiffre понадобилось не так уж много времени.

Криптографы, работавшие над взломом немецких машин Энигма во время Второй мировой войны, тоже пользовались небрежностью врага. Например, многие исходные сообщения начинались с предсказуемых слов и фраз. Ключ представлял собой ряд механических установок, и некоторые встречались чаще других, что было обусловлено физическим расположением элементов управления и «ленью» тех, кто их выбирал. По отдельности ни один из этих недостатков не позволил бы взломать Энигму, но ручеек новых и новых сведений об ошибках при использовании этих машин, несомненно, способствовал их взлому.

Мы не застрахованы от этих проблем даже сегодня. Например, если использовать современные блочные шифры спустя рукава, они могут быть уязвимы к самым разным атакам, начиная с частотного анализа. Передовой алгоритм AES не шифрует каждую букву отдельно, однако шифрование одного и того же блока исходного текста всегда дает одинаковый результат. Намного сложнее анализировать частоту появления блоков данных (которые могут состоять из множества букв), чем отдельных символов, но такой анализ все же возможен. Например, если бы в базе данных (по простоте душевной) записи шифровались по отдельности и если бы они содержали поле «любимая еда ребенка», то среди наиболее часто встречающихся значений была бы зашифрованная версия слова *пицца* (ну уж точно не *брокколи*. Алгоритм AES зашифрует *пиццу* идеально, но то, как мы его использовали, позволит определить это слово, вообще не взламывая шифрование.

«Проблему пиццы» можно решить различными путями, каждый из которых сводится к тонкостям использования AES, а не к изменению самого алгоритма. Например, если к каждой записи в базе данных добавить случайное число, шифротекст, связанный со словом *пицца*, каждый раз будет разным. В более широком смысле, как уже упоминалось ранее, блочные шифры обычно имеют разные режимы работы с разными методиками, направленными на то, чтобы один исходный блок всегда превращался в разные зашифрованные блоки[204].

Выбор криптографического алгоритма и его безопасное использование – это две разные задачи. На сегодня помимо криптографических стандартов, описывающих алгоритмы, у нас есть и стандарты с рекомендациями о способах их применения. *Grande Chiffre* двадцать первого века легко может стать таким же неэффективным, как шифры Наполеона, если использовать его неправильно.

Соблюдение протокола

Криптографические механизмы редко применяются по отдельности. Мы, как правило, следуем какому-то криптографическому протоколу, включающему разные механизмы, каждый из которых обеспечивает определенные аспекты безопасности. Например, при установлении безопасного соединения с помощью протокола TLS ваш браузер использует один механизм для проведения аутентификации сервера, другой – для конфиденциального обмена данными, и еще третий – для проверки происхождения данных (иногда последние два объединены в один). Протокол TLS дает четкие инструкции о том, что, когда и в каком порядке должно произойти. Если хотя бы один этап протокола терпит неудачу, весь процесс должен быть прерван. Например, если сервер не аутентифицирован, протокол TLS должен завершить работу, не установив безопасное соединение.

У Марии Стюарт были катастрофические проблемы с протоколом, поскольку *все* ее механизмы безопасности были скомпрометированы. Она полагалась на алгоритм шифрования, который мог взломать Томас Филиппес. Сургучные печати когда-то использовались для защиты целостности самого зашифрованного текста. Если бы этот механизм работал, Филиппес мог бы по-прежнему справиться с шифрованием, но для этого ему пришлось бы сломать печать, что послужило бы предупреждением для Марии. Однако Артур Грегори умел незаметно снимать сургучные печати, поэтому механизм обеспечения целостности данных тоже не сработал. Но расшифровка текста была еще не самой страшной угрозой. Знания о системе, которыми обладал Филиппес, были настолько полными, что он мог подделать сообщение и выдать его за подлинное.

На завершающих стадиях заговора Филиппесу удалось подделать сообщение от Марии Стюарт к Энтони Бабингтону, в котором он запрашивал имена главных заговорщиков[205]. Читая подлинное с виду сообщение, зашифрованное в точности как было условлено, Бабингтон мог бы ошибочно предположить, что оно пришло от Марии (как вы помните, шифрование не обеспечивает высокую степень целостности данных, такую как проверка происхождения, с которой мы познакомились ранее). Но этот последний провал безопасности ни на что не повлиял, поскольку Бабингтон был арестован и не успел ответить. Через шесть недель он был повешен, потрошен и четвертован, а несколькими месяцами позже головы лишилась и Мария Стюарт.

Даже если механизмы хорошо спроектированного криптографического протокола основаны на устойчивых криптографических алгоритмах, общий уровень защиты может не выдерживать никакой критики, если протокол не соблюдается как следует. Представьте, к примеру, что в протоколе TLS пропущен этап аутентификации сервера, или, что вероятнее, эта задача выполнена неправильно – иными словами, вашему браузеру по какой-то причине не удалось подтвердить, что он взаимодействует с подлинным сервером, к которому вы хотели подключиться. Если в остальном протокол был соблюден, результатом будет установление соединения с мошенническим сервером. Это безопасное соединение не даст стороннему наблюдателю прочитать зашифрованный трафик или модифицировать передаваемые данные, то есть две цели, стоящие перед протоколом TLS, будут достигнуты. Но вы не имеете ни малейшего понятия о том, кто находится с другой стороны взаимодействия[206].

Наверное, главная проблема заключается в том, что разработка хорошего криптографического протокола – задача крайне сложная. Это частично объясняется тем, что взаимодействие различных компонентов может иметь непредвиденные последствия. В качестве примера плохо спроектированного протокола можно привести *WEP* (Wired Equivalent Privacy), который когда-то использовался для защиты сетей Wi-Fi. Он был основан на потоковом шифре под названием *RC4*, который, пожалуй, в момент создания WEP был достаточно устойчивым[207], но…

Архитектура протокола WEP полна недостатков, и одним из самых серьезных можно назвать постоянное изменение ключа шифрования, с помощью которого обеспечивалась конфиденциальность передаваемых сообщений. В замене ключей как таковой нет ничего плохого, но методика, применяемая в WEP, была далека от оптимальной. В итоге злоумышленник, который достаточно долго наблюдал за общением по беспроводному каналу, защищенному с помощью WEP, мог определить главный ключ, который использовался для защиты сети, и в конечном счете расшифровать весь передаваемый трафик[208]. Этот изъян протокола WEP был замечен не сразу, но оказался фатальным. В современных сетях Wi-Fi для защиты информации, которая по ним проходит, применяются протоколы, продуманные более тщательно[209] (если вы используете беспроводное сетевое оборудование, вам лучше проверить, какой протокол в нем выбран, просто чтобы подстраховаться).

Преодоление разрыва

Выбор устойчивых алгоритмов с ключами подходящей длины и применение их в надежных криптографических протоколах – это хороший первый шаг в использовании криптографии на практике. Но это только начало. Благодаря стандартам и тому, что все больше людей понимает важность использования передовых технологий, у современных криптографических систем куда меньше уязвимостей, чем у их предшественниц с менее удачными архитектурами. Но и они не застрахованы от взлома. Проектирование на бумаге – пожалуй, самый простой этап реализации криптографии на практике. Проблемы обычно возникают позже.

Первая проблема – разрыв между проектом и его реализацией. В 1997 году специалист по безопасности Брюс Шнайер поделился своими наблюдениями касательно реализации криптографии, которые остаются актуальными по сей день:

Между математическим алгоритмом и его конкретной реализацией в аппаратном или программном обеспечении существуют огромные

различия. Архитектуры криптографических систем хрупки. Логическая защищенность протокола еще не означает, что он останется безопасным, когда инженер начнет описывать структуру сообщений и передавать биты туда-сюда. «Почти» в этом случае недостаточно; эти системы должны быть реализованы идеально, в точном соответствии с проектом, иначе они не справятся со своими задачами[210].

Аргумент Шнайера состоял в том, что криптографические алгоритмы и протоколы – это особые элементы систем безопасности. Их необходимо реализовывать с большой осторожностью, чтобы архитектура, которую они описывают, воплощалась в точности.

С тех пор мы узнали много нового о том, как создавать безопасные реализации. Мы лучше понимаем, как писать безопасное программное обеспечение и как лучше защитить систему за счет внедрения безопасных аппаратных компонентов. С другой стороны, криптография применяется для все более широкого круга продуктов, и далеко не все разработчики хорошо разбираются в методах безопасной реализации или готовы их использовать. Из-за ограниченного бюджета и сжатых сроков криптография некоторых продуктов имеет заметные изъяны. Как заметил в 2018 году специалист по безопасности Томас Даллиен, «безопасность улучшается, но масштабы небезопасных вычислений растут еще быстрее»[211].

Несмотря на всю накопленную мудрость и примеры ужасных реализаций, между теоретической и практической криптографией по-прежнему остается разрыв.

Беда пришла, откуда не ждали

В декабре 1995 года я, тогда еще неопытный исследователь-криптограф, сидел в душном офисе Аделаидского университета, читая публикации в sci.crypt – одной из ранних новостных интернет-групп, посвященной всему, что связано с криптографией. В то время каждый отдельный человек все еще мог быть осведомлен обо всех направлениях, в которых проводились криптографические

исследования. Работая в государственном секторе, вы даже могли быть знакомы с большинством криптографов.

Статья, привлекшая мое внимание, принадлежала Полу Кохеру (независимому консультанту в сфере безопасности) и называлась «Временной криптоанализ RSA, DH, DSS». Кохер утверждал, что ему удалось взломать RSA и другие алгоритмы с открытым ключом. RSA взломан? Да он спятил! Я продолжил читать:

Я только что опубликовал подробности об атаке, которая многим из вас покажется интересной, поскольку ставит под угрозу немало существующих криптографических продуктов и систем. Основная ее идея в том, что закрытые ключи можно найти, засекая время, необходимое для обработки сообщений[212].

Сомнений не было: Кохер сошел с ума.

Пол Кохер этой статьей объявил о существовании неизвестного неизвестного. Он не взломал алгоритм RSA, который и сейчас остается не менее безопасным, чем в 1995 году, если сделать поправку на увеличение длины ключа в связи с ростом вычислительной мощности. Он утверждал, что реализации RSA, которые ранее считались безопасными, таковыми не являлись. Проблема была не в небрежных ошибках, которые привели к созданию уязвимых реализаций. Кохер поведал о совершенно новом способе атаки на реализации криптографических алгоритмов, явившемся откуда не ждали. И это действительно навсегда изменило практическое применение криптографии.

Кохеру удалось сделать то, что никто за пределами спецслужб не считал возможным. У него был доступ к безопасному – на первый взгляд – устройству, такому как смарт-карта с закрытым ключом RSA. Возможность чтения ключа с таких устройств должна быть исключена, но остается возможным поставить устройству задачу воспользоваться этим ключом для выполнения криптографических вычислений (возьмем для примера вашу кредитную карту: вы не захотите, чтобы продавец мог извлечь ключи, хранящиеся на ее чипе, но вам нужно, чтобы платежный терминал был способен использовать эти ключи для обработки вашей транзакции).

Именно это и сделал Кохер: он заставил устройство произвести вычисления по алгоритму RSA и затем подробно проанализировал то, как это было сделано. В частности, он тщательно измерил разницу во времени выполнения определенных операций, пока устройство пыталось расшифровать разные данные, зашифрованные с помощью RSA. Ловко подобрав шифротекст, который нужно проанализировать, и операции, которые нужно измерить, Кохер в итоге сумел определить закрытый ключ, с помощью которого проводились операции по расшифровке[213]. Потрясающе!

Атаки по времени, проведенные Кохером, открыли новое направление криптографических исследований. Если для получения закрытого ключа достаточно измерить время работы устройства, на котором этот ключ используется, какие еще неожиданные способы подбора ключей могут обнаружиться? А ведь это лишь одна из целого ряда *атак по сторонним каналам*, каждая из которых нацелена на разные аспекты реализации криптографии, и каждая из которых пытается извлечь сведения о закрытых ключах, лежащих в основе криптографических алгоритмов. Среди других примеров можно привести подробный анализ того, сколько электроэнергии потребляет устройство при выполнении криптографических операций, сколько электромагнитной радиации оно излучает, как оно себя ведет в ответ на получение заведомо неверной информации[214].

Для атаки по сторонним каналам обычно требуется наличие устройства, на котором была реализована криптография, чтобы подвергать его «пыткам», пока оно не раскроет свои секреты. В былые времена, когда криптография применялась только на огромных компьютерах, размещенных в специальных подвальных помещениях, атаки подобного рода не вызывали беспокойства. Но сегодня, когда криптография используется даже в карманных устройствах, атаки по сторонним каналам и сопутствующая аналитика представляют реальную угрозу. Если злоумышленнику удастся заполучить ваше устройство, он сможет «допросить» его в попытке выведать ваши секреты.

Вот почему в результате исследований эффективности атак по сторонним каналам были выработаны способы защиты от них. Это тонкие атаки, поэтому и средства борьбы с ними должны быть элегантными. Это еще одно свидетельство (если кто-то до сих пор

сомневался) того, насколько непросто сделать реализацию криптографии безопасной.

Как (на самом деле) спасти мир

Дубль два.

Два агента спецслужб едут в машине, маневрируя по оживленным городским улицам наперегонки со временем. Водитель паникует и срочно связывается со штабом. Пассажир, занудный на вид компьютерщик, только что вставил в свой ноутбук недавно похищенную флешку. «Что на ней?» – спрашивает водитель. «Она зашифрована», – отвечает компьютерщик. «Можешь взломать код?» – спрашивает водитель. Компьютерщик начинает барабанить по клавиатуре, наблюдая за загадочными символами, пляшущими по экрану, прикусывает губу и медленно выдыхает. «Похоже, они используют шифрование AES». – «Но ты можешь его обойти?» – рычит в ответ водитель, пока таймер на экране неумолимо приближается к нулю. «Готово», – спокойно заявляет компьютерщик. «Они использовали стандартный ключ. Вот идиоты», – добавляет он. «Эй, так нечестно!» – сетует водитель. «Мы еще даже не доехали до той крутой сцены с мусоровозом!»

Дубль три.

…«Что на ней?», – спрашивает водитель. «Она зашифрована», – отвечает компьютерщик. «Можешь взломать код?» – спрашивает водитель. Компьютерщик начинает барабанить по клавиатуре, наблюдая за загадочными символами, пляшущими по экрану, прикусывает губу и медленно выдыхает. «Они используют шифрование AES». – «Но ты можешь его обойти?» – рычит в ответ водитель, пока таймер на экране неумолимо приближается к нулю. Компьютерщик, скривившись, снова начинает стучать пальцами по клавиатуре. Тик-так, тик-так, тик-так… Водитель решает срезать и внезапно поворачивает направо, обнаруживая, что путь заблокирован мусоровозом. Раздается свист тормозов, водитель вздыхает в отчаянии. Таймер отсчитывает последние секунды. Компьютерщик, задыхаясь, произносит: «Получилось!». Водитель облегченно улыбается.

«Дружище, ты гений!» – восклицает он. «Вовсе нет, – парирует компьютерщик. – Они добавили в компьютерную программу незащищенный ключ. Я лишь подсмотрел».

Дубль четыре.

…«Что на ней?» – спрашивает водитель. «Она зашифрована», – отвечает компьютерщик. «Можешь взломать код?» – спрашивает водитель. Компьютерщик начинает барабанить по клавиатуре, наблюдая за загадочными символами, пляшущими по экрану, прикусывает губу и медленно выдыхает. «Они используют шифрование AES». – «Но ты можешь его обойти?» – рычит в ответ водитель, пока таймер на экране неумолимо приближается к нулю. Компьютерщик, скривившись, снова начинает стучать пальцами по клавиатуре. «Похоже, ключ сгенерирован из пароля. Дайте мне минуту». Тик-так, тик-так, тик-так… Водитель решает срезать и внезапно поворачивает направо, обнаруживая, что путь заблокирован мусоровозом. Раздается свист тормозов, водитель вздыхает в отчаянии. Таймер отсчитывает последние секунды. Компьютерщик, задыхаясь, произносит: «Получилось! Эти выскочки всегда используют пароли вроде „Хавьер Бардем“»[215].

Обращайтесь с ключами как следует!

Хороший алгоритм – есть. Надежный протокол – есть. Тщательная реализация – есть. Защита от атак по сторонним каналам – есть. Ничего не забыли?

Осталось еще кое-что. Криптография, как вы уже прекрасно знаете, опирается на ключи. Если предположить, что алгоритмы спроектированы и реализованы правильно, задача по защите данных превращается в другую, чуть менее сложную задачу, состоящую в безопасном хранении ключей. Если криптография справилась с тем, чего мы от нее хотели, нам нужно как следует позаботиться о ключах[216].

К ключам можно относиться как к живым существам. Они рождаются, проживают свой срок и затем умирают. На протяжении

жизненного цикла ключа его следует взращивать. Этот цикл состоит из ряда важных стадий. Сначала ключи *генерируются* (создаются). Затем они *распространяются* между теми членами криптографической системы, которым они нужны. Дальше они обычно *хранятся* в ожидании момента, когда ими воспользуются. В некоторых системах ключи должны регулярно *сменяться*. В конечном счете необходимость в них пропадает, и их нужно *уничтожить*.

Со всеми стадиями жизненного цикла криптографического ключа необходимо обращаться с осторожностью, поскольку неправильная работа хотя бы одной из них может привести к сбою всей криптосистемы. Здесь действуют те же правила, что и с ключом от входной двери. Если ключ слишком простой, любой, у кого есть металлическая скрепка, сможет взломать замок. Нечистоплотный агент по недвижимости может передать дубликат вашего ключа преступникам. Если вы оставите свой ключ под цветочным горшком у ворот, кто-то может его найти и воспользоваться. Если в ваш дом вломится вор, а вы после этого не смените замки, он может вернуться и украсть вещи, которые вы купили на деньги страховой выплаты взамен похищенных.

Если не обращаться с криптографическими ключами подобающим образом, могут возникнуть две фундаментальные проблемы. Прежде всего, ключ, который должен был оставаться в тайне (например, ключ симметричного шифрования, закрытый ключ для асимметричной расшифровки или ключ для цифровых подписей), может быть раскрыт. В сценарии нашего вымышленного фильма мир был (на самом деле) спасен тремя способами, каждый из которых сработал в результате раскрытия ключа из-за неправильного обращения с ним на разных стадиях его жизненного цикла. В первом случае мы видели неправильную генерацию ключа (с использованием слабого пароля). Во втором – неправильное его хранение (добавление ключа в код программы). В третьем злоумышленники не удосужились сменить стандартный ключ на собственный, заново сгенерированный[217]. Если на какой-либо стадии жизненного цикла ключа вы не сумеете сохранить его в тайне, последствия могут быть катастрофическими (или наоборот, спасти мир, смотря на чьей вы стороне). Необходимость защиты секретных ключей кажется очевидной, ведь то же самое относится и к физическим ключам.

Вторая фундаментальная проблема состоит в том, что криптографический ключ может быть предназначен не для того, чего вы ожидали, или принадлежать не тому, о ком вы думали. Для этого аспекта не так просто найти соответствие в мире настоящих ключей. Но давайте попробуем.

Представьте, что вы находитесь в бегах и встречаете знакомого, который предлагает вам ночлег. Знакомый дает вам свой адрес и ключ от входной двери. Вы находите дом, открываете дверь и вдруг понимаете, что перед вами стойка регистрации местного отделения полиции. Ваш знакомый оказался полицейским под прикрытием! Хм-м… Почему такая ситуация кажется маловероятной?

Вы не заметили на здании дружественную вывеску «Полиция» и не обратили внимания на служебные автомобили характерной окраски, припаркованные вокруг. Но важней всего то, что физические ключи должны передаваться лично, и контекст дает некоторое представление об их назначении. Когда продавец в автосалоне вручает вам ключи от только что купленной машины и направляет вас к новенькой «BMW» на стоянке, есть веские основания полагать, что это и правда ключи от машины. Конечно, может оказаться, что они не от «BMW» и что ржавый фургон, припаркованный рядом, приветственно подмигивает вам фарами, а продавец тем временем стремительно удирает. Это *могло бы* случиться. Но обычно этого не происходит.

Криптографические ключи – виртуальные объекты, поэтому им недостает контекста. Когда вы подключаетесь к удаленному сайту, и браузер предлагает вам воспользоваться его открытым ключом шифрования, чтобы начать установление защищенного канала связи, откуда вы *знаете*, что этот открытый ключ действительно принадлежит этому сайту[218]? Когда друг присылает вам по электронной почте открытый ключ, чтобы вы могли послать ему зашифрованное сообщение, откуда вы *знаете*, что злоумышленник не перехватил его письмо и не заменил его ключ своим? Когда вы покупаете дешевую криптографическую штуковину у руританской компании, откуда вы *знаете*, что копии ее криптографических ключей не хранятся в базе данных правительства Руритании?

Основная задача управления ключами (key management) состоит в том, чтобы хранить секретные ключи действительно в секрете и гарантировать, что мы используем подходящие ключи в правильном

контексте. Это, пожалуй, самый сложный аспект практического применения криптографии в реальных системах, так как он выступает связующим звеном между самой криптографической технологией и организациями/людьми, которым нужно ее использовать.

Хорошие и плохие ключи

Наверное, самым тонким этапом управления ключами является их генерация. Поскольку в симметричной и асимметричной криптографии она выполняется немного по-разному, рассмотрим эти случаи отдельно.

Безопасность симметричного криптографического алгоритма основана на предположении о том, что симметричные ключи сгенерированы случайным образом. У этой идеи есть две проблемы.

Первая: генерировать случайные ключи непросто. На самом деле само понятие «настоящей случайности» вызывает бурные споры между философами и физиками, от которых я предпочту держаться подальше, по крайней мере в этой книге[219]. По-настоящему случайные числа (они же *недетерминистические* случайные числа) обычно берутся из «естественного» физического источника. Один из самых очевидных способов сгенерировать недетерминистическую случайность состоит в подбрасывании монеты. Если предположить, что монета сбалансирована, а подбрасывающий ее человек непредвзят, каждый результат будет независимым физическим событием, и орел будет выпадать с той же вероятностью, что и решка. Это отличный способ сгенерировать случайный ключ: мы можем закодировать орел как 1, а решку как 0, в результате чего получится криптографический ключ, каждый бит которого не зависит от предыдущих и последующих[220]. С другой стороны, этот способ чудовищно непрактичен для большинства криптографических задач. *Хотите купить что-нибудь на моем веб-сайте? Будьте так добры, подбросьте сначала монетку 128 раз, чтобы сгенерировать ключ AES.*

К счастью, недетерминистические случайные числа можно генерировать и из других физических источников, не требующих человеческого вмешательства. Подойдут такие явления как белый шум,

атмосферные колебания и радиоактивный распад. Их можно так или иначе измерить, а результаты преобразовать в ноли и единицы[221]. Это достаточно эффективный, хотя и немного обременительный подход. Если у вас есть доступ к такому физическому устройству, и вы можете извлечь из него по-настоящему случайные данные, вам повезло. Но что делать тем, у кого такого доступа нет?

У генерации недетерминистических ключей есть еще один недостаток. С помощью такого рода методов нельзя сгенерировать два идентичных случайных ключа в двух разных местах. Действительно, весь смысл генерации недетерминистических случайных чисел в том, что таких совпадений *не* должно происходить. Подбрасывание монеты является отличным источником случайных значений именно потому, что результат непредсказуем. Однако во многих ситуациях, в которых применяется симметричная криптография, мы, наоборот, *хотим* получить два идентичных ключа. Когда вы кому-то звоните, ваш телефон и ваш сотовый оператор должны использовать общий ключ, чтобы зашифровать ваш разговор.

Когда дело принимает крутой оборот, что делают крутые? Они, конечно же, жульничают. Как мы уже не раз обсуждали, вывод хорошего криптографического алгоритма должен казаться «случайным», поэтому криптография сама по себе является потенциальным источником «случайных» данных. Во время звонка ваш телефон и сотовый оператор используют определенный криптографический алгоритм, чтобы сгенерировать новый «случайный» симметричный ключ, с помощью которого можно зашифровать ваш разговор. У телефона и оператора уже есть долгосрочный симметричный ключ, хранящийся на вашей SIM-карте (который вполне мог быть сгенерирован недетерминистическим путем). Этот ключ подается на вход криптографическому алгоритму, который затем возвращает новый общий ключ. Телефон и оператор используют одинаковые ввод и детерминистский алгоритм, чтобы сгенерировать один и тот же ключ. Поскольку этот процесс детерминирован и, как следствие, воспроизводим в двух разных местах, результат нельзя считать по-настоящему случайным. Вместо этого мы называем его *псевдослучайным*.

Ключи, сгенерированные псевдослучайным образом, может, и нельзя считать по-настоящему случайными, но для большинства

криптографических задач их достаточно. Ключ, полученный из *генератора псевдослучайных чисел* (основанного на криптографическом алгоритме), может оказаться таким же устойчивым к подбору, как и ключ, сгенерированный путем подбрасывания монеты. Но это лишь *потенциальная* возможность.

За прошедшие годы низкокачественные генераторы псевдослучайных чисел не раз оказывались слабым местом криптосистем. Эту уязвимость, вероятно, допускают по недосмотру. В рекламе средств безопасности часто говорится об использовании «передового 128-битного шифрования AES», но мало кто хвастается тем, как генерируются ключи. Плохой генератор псевдослучайных чисел неспособен создавать ключи, случайные хотя бы на вид. Злоумышленник может проанализировать такой генератор и обнаружить, что некоторые ключи не генерируются никогда или встречаются чаще других. Если вы захотите отыскать неизвестный вам секретный ключ полным перебором, эта информация будет крайне полезной[222].

Как мы уже отмечали, крупные случайные числа сложно запомнить, поэтому для псевдослучайной генерации ключей иногда используют пароли. Вы вводите пароль, а генератор псевдослучайных чисел преобразует его в криптографический ключ. Если не проявить в ходе этого процесса максимальную осторожность, могут возникнуть разнообразные проблемы. Например, ключи, полученные из распространенных паролей, могут генерироваться чаще других, тогда как ключи на основе крайне редких паролей могут вообще никогда не встречаться. На этот случай криптографы создали специальные *функции формирования ключей* – алгоритмы, предназначенные для генерации ключей из более простых данных, вроде паролей[223].

Асимметричная криптография включает еще более сложный процесс генерации ключей, поскольку асимметричные ключи – это не «просто случайные» числа. В спецификации любого асимметричного алгоритма есть информация о том, как сгенерировать необходимые ключи. Если придерживаться этих инструкций, никаких проблем возникнуть не должно. К сожалению, люди славятся пренебрежительным отношением к инструкциям, особенно если те кажутся сложными. Результаты расследования многих происшествий показывают, что разработчики просто не соблюдали спецификацию и

генерировали некачественные ключи. Например, согласно исследованиям, подавляющее большинство открытых ключей RSA в Интернете имеют общие свойства (в частности, в них используются одинаковые простые множители), что делает их небезопасными[224]. Это не совпадение, а явный признак того, что ключи генерировались не по правилам.

На сегодня большинство людей не занимаются созданием собственных криптографических алгоритмов (похоже, разработчики наконец прислушались к рекомендациям). Но лишь немногим из них хватает здравого смысла не придумывать собственные способы генерации ключей на коленке.

Нужный ключ в нужное место

Одна из важнейших стадий управления ключами – их передача и распространение, и мы уже уделили этому процессу немало внимания. На первый взгляд все просто: он состоит в том, чтобы доставить правильный ключ по правильному адресу.

Если доставить нужные ключи не туда, куда нужно, это явно создаст проблемы, поэтому никакое внимание, уделенное распространению ключей, не будет лишним. Более того, для этого разработано немало разных методик. Как уже говорилось, во многих случаях ключи распространяются прямо в процессе производства, когда их предустанавливают на устройства (такие как мобильные SIM-карты, брелоки автомобильной сигнализации и т. д.). Иногда распространение ключей не вызывает никаких сложностей, поскольку устройства, которым нужны общие ключи, находятся в непосредственной близости друг от друга (например, вы можете прочитать ключ на нижней крышке маршрутизатора и ввести в устройство, которое подключаете к домашней сети Wi-Fi). В системах с централизованным управлением ключи могут безопасно распространяться с помощью пристально контролируемых процессов и средств управления. Банки выработали высокозащищенные процедуры распространения ключей, которые используются в аппаратном обеспечении банкоматов, банковских карт клиентов и т. д.

Как только один и тот же ключ доставлен двум сторонам, дальнейших хлопот с его распространением чаще всего можно избежать, если использовать специальную функцию для формирования из него нового ключа. Ваш сотовый оператор встроил ключ в SIM-карту, которую вы приобрели со стартовым пакетом. Каждый раз, когда вы кому-то звоните, ваш разговор шифруется с помощью совершенно нового ключа, который основан на ключе из вашей SIM-карты. Оригинальный ключ известен как абоненту, так и сотовому оператору, поэтому обе стороны могут независимо друг от друга сформировать из него один и тот же новый ключ; больше не нужно ничего распространять. Этот новый ключ используется для шифрования звонка и затем отбрасывается. При следующем звонке на основе ключа вашей SIM-карты будет создан совершенно новый ключ[225].

Распространять ключи сложнее, когда стороны взаимодействия находятся в открытой системе, такой как Интернет, физически далеко друг от друга, и до сих пор не вступали ни в какие деловые отношения, в ходе которых могли бы обменяться ключами. Обычно что-то такое происходит, когда вы делаете покупки в интернет-магазине или инициируете общение с новым контактом WhatsApp. Я уже отмечал, что именно такого рода ситуации мотивируют применение асимметричного шифрования. Гибридная криптография предоставляет механизмы распространения симметричных ключей под защитой асимметричного шифрования. Еще одним широко известным подходом к распространению ключей в таких случаях является *протокол Диффи – Хеллмана*, который позволяет двум сторонам послать друг другу свои открытые ключи, на основе которых затем можно сформировать общий закрытый ключ[226].

Избежать доставки корректных ключей не по назначению – это лишь полдела. Не менее насущная задача – предотвращение доставки некорректных ключей в нужное место. Я упоминал об этом при обсуждении недостатков асимметричного шифрования, когда говорил, насколько важно позаботиться о том, чтобы открытый ключ был провязан к его настоящему владельцу. Если такой связи нет, преступник может создать правдоподобную копию настоящего веб-сайта, подсунуть вам собственный открытый ключ вместо подлинного и затем похитить реквизиты вашей банковской карты, когда вы, ничего не подозревая, пытаетесь за что-то заплатить. Нам нужен механизм,

гарантирующий, что предоставленный вам открытый ключ принадлежит именно тому сайту, на который, как вам кажется, вы вошли.

Стандартным средством привязки открытого ключа к его владельцу является *сертификат открытого ключа*. По сути, это подтверждающий документ вроде тех сертификатов, которые многие вешают на стену. У меня дома на стене висят такие сертификаты:

Настоящий сертификат подтверждает, что Кайла сдала экзамен по игре на гитаре за второй класс с отличием.

Настоящий сертификат подтверждает, что Финлэй выиграл чемпионат класса по внимательному слушанию.

Настоящий сертификат подтверждает, что Рамон прошел курс дрессировки взрослых собак.

Сертификат открытого ключа фактически говорит следующее: *Настоящий сертификат подтверждает, что открытым ключом веб-сайта* ***www.reallycheapwidgets.com*** *является X*, где X – это действительный открытый ключ (настолько длинный, что я не стану приводить его здесь целиком)[227].

Сертификаты делают громкие заявления, но все упирается в то, кто на самом деле эти заявления делает. Если вернуться к сертификатам на моей стене, в первом случае это исполнительный директор объединенного совета Королевской школы музыки; во втором – директор начальной школы Катберта Линдисфарнского; в третьем – Сара Хикмотт, бакалавр наук (с отличием), профессиональный тренер из Pet Necessities. Кому принадлежат эти заявления? Важным людям. Людям, которые должны знать, о чем говорят. Каждая из упомянутых сторон имеет определенный авторитет и пользуется уважением в своей сфере.

Точно так же сертификаты открытого ключа должны быть созданы теми, кто может подтвердить связь между открытым ключом и его владельцем и кому мы можем доверять. В киберпространстве эту роль играет *центр сертификации*; эту роль может играть как официальный орган (скажем, правительство), так и коммерческий поставщик услуг

сертификации[228]. Любой, кто полагается на открытый ключ, должен иметь основания доверять центру сертификации. Если вы не верите, что этот центр добросовестно выполняет свои обязанности, вам не стоит доверять информации, указанной в сертификате. Все просто.

Одна из распространенных ошибок состоит в придании сертификату слишком большого значения. Сертификат подтверждает только то, что в нем написано, и ничего больше. Финлэй может быть суперслушателем в школе, но сохраняет ли он ту же концентрацию дома? Рамон[229] прошел курс дрессировки, но научился ли он там чему-то (или только узнал, что ему нравится сыр)? Тот факт, что в момент подписания сертификата открытым ключом веб-сайта **www.reallycheapwidgets.com** является X, не означает, что этот ключ будет действителен по истечении какого-то срока, что его можно использовать для шифрования финансовых данных или что угодно еще. Чтобы решить некоторые из этих вопросов, сертификаты открытого ключа обычно содержат дополнительную информацию. Но даже самые подробные из них – не более чем набор фактов, касающихся открытого ключа. Они не дают гарантий или ответов на более глубокие вопросы – например, был ли открытый ключ изначально сгенерирован безопасным образом[230].

Надежность сертификата определяется качеством механизмов обеспечения целостности, которые его защищают. Сертификат Кайлы напечатан на торжественном пергаменте, украшен различными официальными логотипами, на нем даже есть водяной знак (на двух других – цветные изображения сургучных печатей). Сертификат открытого ключа – виртуальный объект, для обеспечения его целостности необходимо криптографическое решение. Вместо печати центр сертификации использует цифровую подпись. Тот, кто полагается на информацию в сертификате открытого ключа, должен ее проверить, чтобы убедиться в подлинности содержимого. Для этого нужен открытый проверочный ключ, созданный центром сертификации. Поскольку мы должны быть *уверены* в происхождении этого открытого ключа, он должен быть привязан к центру сертификации средствами еще одного сертификата. Но кто его подписывает?

Когда вы покупаете что-нибудь в каком-то дисконтном интернет-магазине наподобие **www.reallycheapwidgets.com**, большую часть

работы с сертификатами открытого ключа берет на себя ваш браузер. Прежде чем начинать торговлю, владелец магазина должен получить сертификат открытого ключа от общепризнанного центра сертификации. Открытый ключ этого центра был сертифицирован вышестоящей инстанцией. Ваш веб-браузер содержит проверенные сертификаты *корневых* центров сертификации[231]. Когда интернет-магазин присылает свой сертификат открытого ключа вашему браузеру, тот сверяет его со всеми подходящими сертификатами, которые в него установлены. Если все хорошо, ваша транзакция проходит без проблем. Если хотя бы одна проверка оказывается неудачной, браузер может выдать вам предупреждение и уточнить, действительно ли вы желаете продолжать работу с этим сайтом. Таким образом браузер фактически информирует вас о невозможности подтвердить, что вы действительно взаимодействуете с настоящим веб-сайтом **www.reallycheapwidgets.com**. Вы сами решаете, продолжать или нет, но, как правило, из соображений безопасности соединение лучше разорвать[232].

Надеюсь, я достаточно отвлекся на управление открытыми ключами, и чтобы продемонстрировать, как сертификаты позволяют удостоверить настоящего владельца открытого ключа, и чтобы показать, что сертификация – дело тонкое, требующее проведения множества управленческих процедур. Я не рассказал, *как* центр сертификации может идентифицировать владельца открытого ключа, и не стал останавливаться на том, что происходит, когда содержимое сертификата нужно изменить. Поддержка сертификатов открытого ключа требует возведения вокруг них полноценной инфраструктуры, которая решает такие проблемы[233].

Распространение ключей имеет свои сложности, справиться с которыми можно множеством разных способов. Все эти решения работают, если их тщательно подобрать и реализовать. Именно поэтому мы ежедневно используем криптографию.

Не криптографией единой

Вспомним, что происходит с данными во время шифрования: данные… данные… <шифрование – бабах!> зашифрованные данные… зашифрованные данные… <расшифровка – бабах!> данные… данные… Иными словами, между первым и вторым бабахом данные защищены шифрованием. Но перед первым и после второго они у всех на виду.

Звучит как нечто очевидное. Когда данные не зашифрованы, они незашифрованы. Вот так открытие! Однако криптографическая защита нередко дает сбой именно потому, что нам не удается определить, когда и где данные находятся в незашифрованном виде.

Наглядной иллюстрацией значимости *безопасности в конечной точке* может послужить защита веб-соединений с помощью протокола TLS. При оплате товара в интернет-магазине вы практически наверняка используете TLS для шифрования сведений о транзакции. Этот протокол шифрует информацию, такую как реквизиты вашей банковской карты, между вашим браузером и сервером магазина. Но это шифрование начинается не в момент ввода данных с клавиатуры. Данные могут находиться в оперативной памяти или храниться на жестком диске. Их может заполучить любой, кто стоит рядом и видит, что вы вводите, или кто имеет доступ к вашему компьютеру или может запустить на нем какую-то программу, или даже тот, кто установил кейлоггер на вашу клавиатуру, чтобы записать нажатия клавиш. А уж кто получает к ним доступ на стороне сервера, можно только догадываться. Некоторые сайты хранят платежную информацию в базе данных; это означает, что ваши реквизиты может получить любой, у кого есть доступ к этой базе. Интернет-магазины должны беречь эти данные с большой осторожностью (используя криптографию, конечно), но рассчитывать на это как на гарантию нельзя[234].

Когда судебные следователи сталкиваются с зашифрованными данными, они не сдаются и не расходятся по домам. Им прекрасно известно, что данные зачастую находятся где-то рядом, иногда в неожиданных местах – как до шифрования, так и после расшифровки. Наивный обыватель, пытающийся спрятать какую-то информацию на своем ноутбуке, может зашифровать файл и удалить оригинал. На первый взгляд, в папке остаются только зашифрованные данные. Однако удаление не означает полное уничтожение; эта операция просто разрывает связь между самим файлом и названием, по

которому его идентифицирует система. Обладая достаточной квалификацией, вы можете порыться в ноутбуке и извлечь безымянный «удаленный» файл[235].

Как уже отмечалось во время третьего дубля сцены, в которой секретный агент наперегонки со временем отчаянно пытается спасти мир, есть еще один фрагмент информации, который может быть небрежно оставлен в конечной точке – криптографический ключ. Конечно, ключи лучше всего хранить на специальных защищенных устройствах. В качестве легковесного примера можно привести смарт-карты вроде тех, что используются банками и сотовыми операторами. Если вам нужно что-то потяжелее, можете воспользоваться *аппаратными модулями безопасности* (англ. hardware security modules или HSM) – это специальное оборудование для хранения и администрирования ключей[236]. Извлечь ключ из защищенного устройства непросто. Но если вы решите не заморачиваться и прибегнете к намного более дешевому варианту – предпочтете хранить ключи прямо в программном обеспечении, – то с помощью подробного анализа конечной точки их можно будет обнаружить и расшифровать данные.

Специалист по компьютерной безопасности Джин Спаффорд однажды метко подметил: «Использование шифрования в Интернете – это то же самое, что использовать бронированный автомобиль для доставки реквизитов кредитной карты от человека, живущего в картонной коробке, к тому, который ночует на скамейке в парке»[237]. Шифрование работает, но большую часть своего времени в киберпространстве вы все равно находитесь в положении бездомного.

Углеродная форма безопасности

Специалисты по кибербезопасности известны своими (наверное, слишком частыми) заявлениями о том, что «самым слабым звеном» в любой системе безопасности, включая криптосистемы, является человек[238]. Это утверждение подразумевает, что большинство происшествий в этой сфере происходит из-за небрежности или глупости людей, пользующихся системой. Вы выбрали лучший

алгоритм, идеально его реализовали, обеспечили наивысшие стандарты управления ключами – и все ради чего? Чтобы какой-то дурак записал свой ключ на стикере и приклеил его к монитору?

Увы, такое бывает, и не так уж редко. Однако утверждение, что люди – самое уязвимое место криптосистемы, вызывает довольно серьезные вопросы. Кто кому служит в этой ситуации? Если на время забыть о мрачном видении будущего, большинство технологий создаются на благо людей. Намекая на то, что люди недостаточно хороши для этих технологий, мы фактически признаем, что хвост виляет собакой. А из этого следует еще более важный вывод: если взаимодействие между человеком и криптосистемой действительно является точкой, где все с большой долей вероятности может пойти наперекосяк, то, очевидно, система должна быть готова противостоять этой уязвимости. Взаимодействие с человеком должно быть организовано так, чтобы не давать поводов для сожалений.

Какого рода криптографические бедствия могут спровоцировать пользователи в конечной точке криптосистемы? Они могут зашифровать файл безопасным образом, сохранить его незашифрованную копию на флешку и потерять ее в автобусе по дороге домой. Они могут забыть зашифровать конфиденциальные материалы или нечаянно выключить шифрование. Они могут записать на клочке бумаги пароли для генерации криптографических ключей. Они могут одолжить смарт-карты с криптографическими ключами (банковские карты, пропуска с работы, удостоверения) своим друзьям. Они могут зашифровать данные на своем ноутбуке и потерять ключ. Они могут уйти на обед, бросив без присмотра аутентифицированное устройство, которым может воспользоваться любой, кто проходит мимо. Глупые, глупые люди… Что же делать?

От ошибок и некомпетентности никуда не деться. Лучший способ борьбы с этими угрозами – несомненно, полный отказ от взаимодействия с человеком при использовании криптографии. Неплохой пример – защита телефонных звонков. Вы набираете номер, и телефон соединяется. Вы даже не замечаете, что в этом процессе используется криптография. То же самое касается многих других привычных нам технологий, таких как системы обмена сообщениями в Интернете. Криптографические операции выполняются автоматически, без вмешательства человека.

Неочевидный риск, возникающий вследствие автоматизации криптографии, состоит в том, что мы заодно избавляемся от взаимодействия между людьми и устройством, которое могло бы быть *желательным* с точки зрения безопасности. Например, незримые криптографические действия, происходящие между ключом и дверью вашего автомобиля, не требуют от вас ничего, кроме наличия этого ключа в вашем кармане. Риск неправильного использования криптографии человеком сводится к минимуму; такая схема даже обеспечивает определенную гибкость, поскольку воспользоваться автомобилем может любой, кто одолжит у вас ключи. Но это также означает, что любой, кто украл эти ключи, получит все необходимое для того, чтобы открыть машину и уехать на ней куда угодно.

В вопросах доступа к своему банковскому счету вам, наверное, не захочется играть настолько пассивную роль. Вот почему для работы криптографических механизмов, лежащих в основе интернет-банкинга, обычно требуется взаимодействие с человеком – хотя бы в виде предоставления PIN-кода, пароля, биометрической информации, кода доступа, пришедшего на телефон, и т. д. Эти фрагменты данных усиливают безопасность, привязывая криптографические операции к человеку вместо того, чтобы просто обрабатывать токен безопасности вроде смарт-карты или аутентификатора. Однако вовлечение в процесс людей создает в системе новую точку уязвимости, ведь людям свойственно терять, забывать, а то и просто отдавать свои вещи кому ни попадя.

Автоматическое применение криптографии создает и некоторые менее очевидные проблемы. Представьте, к примеру, что организация, которая раньше разрешала сотрудникам шифровать свои ноутбуки добровольно, перешла на централизованную систему с обязательным шифрованием. На первый взгляд, это позволило исключить утечку информации с незашифрованных ноутбуков. Но вместе с тем возникла потенциально более серьезная уязвимость: если организация решит использовать единый главный ключ для шифрования всех ключей на каждом устройстве, это ставит под угрозу данные на *всех* ноутбуках сразу, ведь главный ключ может быть раскрыт[239].

Возьмем еще один пример. Применение системы обмена сообщениями с автоматическим шифрованием может привести к тому, что пользователь перестанет задумываться, какую информацию ему

следует или не следует передавать по этой системе. Если в ходе расследования у него изымут телефон, и на нем окажутся незашифрованные данные, по ним можно будет восстановить переданную информацию. Как ни странно, в этом случае автоматизация шифрования может *снизить* объем данных, остающихся конфиденциальными.

Но иногда в криптографическом процессе никак не обойтись без участия человека. Вы, скорее всего, не шифруете каждый вложенный файл, который отправляется по электронной почте. Однако время от времени необходимость в отправке конфиденциального вложения все же возникает. В таких случаях вам нужно каким-то образом активировать шифрования – либо через расширение вашего почтового клиента, либо с помощью отдельного средства шифрования, установленного на вашем компьютере. Такая активация требует от вас определенных действий. К сожалению, людям, которые плохо разбираются в компьютерах или криптографии, будет сложно воспользоваться криптографическими продуктами[240]. Пользователи нередко бросают попытки зашифровать данные, запутавшись в непонятных терминах и загадочных инструкциях. Людей не стоит считать слабым звеном априори, но запутавшийся человек может стать таковым.

Криптография должна служить человеку, а не наоборот. В безопасной криптосистеме взаимодействие между криптографическими механизмами и живыми пользователями должно учитываться еще при проектировании; для этого нужно либо минимизировать взаимодействие с человеком, либо доступно объяснить, как и зачем выполнять тот или иной шаг[241]. В действительности же самым слабым звеном в криптосистеме является неспособность учесть то, как с ней будут взаимодействовать пользователи.

Правильное применение криптографии на практике

Учитывая разнообразие потенциальных проблем, представленных выше, вам может показаться, что криптографию невозможно

достаточно хорошо реализовать на практике. Все эти потенциальные угрозы необходимо осознавать, но сам вердикт не вполне справедливый. Корректное применение криптографии – задача, может, и непростая, но выполнимая, хотя и требующая осторожности.

По крайней мере такая задача стоит потраченных усилий. Некоторые утверждают, что плохо реализованная криптография хуже, чем ее полное отсутствие, так как она дает обманчивое чувство защищенности[242]. Во многих контекстах с этим аргументом сложно не согласиться. Но несмотря на то что криптографию сложно заставить работать корректно, лучше попытаться это сделать, чем сдаться, даже не попробовав. В конце концов, даже шифр Цезаря позволит вам прикрыть свои тайны от большинства людей.

Да и поводов для оптимизма достаточно. Мы как общество проектируем все более совершенные криптографические алгоритмы и протоколы. Мы улучшили наши навыки проектирования и реализации безопасности. Мы разработали стандарты для безопасного обращения с криптографическими ключами. Мы стали намного опытней во внедрении криптографии и извлекли уроки из прошлых ошибок. В целом мы знаем, *как* правильно использовать криптографию; нам лишь нужно применять наши знания на практике!

Корректное применение криптографии требует понимания криптосистемы, которая окружает криптографические алгоритмы и ключи. Нам нужно правильно реализовать каждый ее элемент без исключения. Лучшим свидетельством этого является информация, раскрытая Сноуденом в 2013 году и описавшая различные способы использования криптографии в киберпространстве, которые *не* работают. Каким бы ни было ваше мнение об этичности поступка Сноудена, его откровения послужили полезным напоминанием о том, что для обхода защиты, которую предлагает криптография, достаточно найти в криптосистеме *одно* слабое место. Таких потенциальных мест много, и они редко имеют отношение к самой криптографии.

8. Дилемма криптографии

Из всех механизмов безопасности, которые предлагает криптография, самым политически спорным остается шифрование, так как оно защищает конфиденциальность информации. У всех нас есть секреты, но нам этого недостаточно – мы хотим знать, что скрывают другие. Однако вопрос о том, что должно или не должно быть конфиденциальным, субъективен, и ответ на него может меняться со временем. Мы все, наверное, согласны с тем, что личные финансовые данные должны храниться в тайне. Но заслуживает ли такой конфиденциальности корпорация, которую обвиняют в злостном уклонении от налогов? Такого рода конфликты порождают социальные дилеммы, которые только подогревают политические споры об использовании криптографии.

Проблематичность криптографии

Надеюсь, вы согласитесь с тем, что криптография чрезвычайно полезна. Являясь основой безопасности, она позволяет нам проделывать в киберпространстве потрясающие вещи. Однако криптография не всегда используется во благо. Вот по меньшей мере шесть потенциально нежелательных ситуаций.

1. Понимая, чем чреваты незащищенные данные, уходя в отпуск, вы шифруете все содержимое своего ноутбука. Спустя три недели под жарким солнцем вы возвращаетесь отдохнувшим и полным сил. К сожалению, вы так хорошо расслабились, что не можете вспомнить фразу-пароль, из которой был получен ключ для шифрования. Без пароля нет ключа, без ключа нет данных.
2. Вы включаете свой домашний компьютер и видите на экране следующее сообщение: *Ой, ваши файлы были зашифрованы! Ваши многочисленные документы, фотографии, видеоролики, базы данных и прочие материалы теперь недоступны. Не теряйте время попусту, пытаясь их восстановить. Никто не сможет их расшифровать без*

нашего ключа. У вас есть три дня на то, чтобы отправить выкуп (только в биткоинах), а потом ваши файлы будут утеряны навсегда! Ужас! Вы подцепили *вирус-вымогатель* – мерзкую программу, которая и правда зашифровала все ваши файлы. И теперь кто-то требует от вас деньги в обмен на ключ, необходимый для их расшифровки[243].

3. Вы – системный администратор, который сконфигурировал правила, определяющие, какой интернет-трафик может поступать в вашу сеть. У вас есть черный список веб-адресов, ключевых слов и вредоносного ПО. Любые внешние соединения проверяются на наличие какой-либо связи с содержимым черного списка; если такая связь имеется, соединение отклоняется. Однажды вы с досадой обнаруживаете, что известная вредоносная программа уже заразила многих пользователей вашей системы. Как ей удалось обойти ваши проверки?! По всей видимости, она была зашифрована, и это позволило скрыть ее природу достаточно хорошо, чтобы она просочилась через ваши защитные механизмы.

4. Вы – детектив, расследующий убийство. Вы изъяли у подозреваемого телефон, на котором, как вам кажется, находятся инкриминирующие фотографии. К сожалению, вам недоступны никакие изображения, хранящиеся на этом телефоне, поскольку подозреваемый их зашифровал. Вы уверены, что эти фотографии – ключевая улика в деле, но у вас попросту нет возможности их просмотреть[244].

5. Вы – следователь, изъявший веб-сервер с непристойными изображениями детей. По записям в журнале видно, что у этого сервера было много регулярных посетителей, которых вам бы хотелось привлечь к ответственности. К сожалению, все они использовали криптографическое программное обеспечение Tor, которое затрудняет их выслеживание. Кто они? Где они?[245]

6. Вы – офицер разведки, следящий за ячейкой потенциальных террористов. Вам удалось получить доступ к телефону одного из подозреваемых. Тот переговаривается с сообщниками в системе обмена сообщениями, известной своей надежной криптографической защитой. Вы видите, что подозреваемый регулярно контактирует с другими членами ячейки, но у вас нет возможности узнать, о чем они разговаривают[246].

Как видно из этих примеров, у криптографии есть всего две проблемных функции. Конфиденциальность позволяет скрыть данные кому угодно, в том числе шантажистам, убийцам и террористам. Благодаря анонимности в киберпространстве любой может скрыть свою личность, в том числе и те, кто представляет угрозу для детей. Когда криптографию упоминают в новостях, речь обычно идет не о хеш-функциях, имитовставках, цифровых подписях или идеальных паролях. Жаркие дискуссии вокруг криптографии неизменно сводятся к использованию шифрования, так как помимо защиты секретов оно может применяться для создания технологий наподобие Tor, обеспечивающих анонимность.

Дилемма

Давайте проанализируем причины проблем, которые вызывает шифрование в наших шести примерах. Первые три существенно отличаются от остальных.

В первом случае описывается единственная ситуация, которая возникла случайно и не была преднамеренным актом. Вы забыли пароль, необходимый для расшифровки вашего диска. Такая оплошность может оказаться катастрофической, но стоит ли винить криптографию? Мне так не кажется; это была ваша ошибка. Шифрование диска приносит больше пользы, чем вреда, но у него есть один нюанс: чтобы получить доступ к данным, нужно помнить ключ. Этот ключ настолько важен, что у вас должны быть предусмотрены процедуры, которые исключают его потерю. Если вы плохо запоминаете пароли, его стоит хранить в надежном месте на отдельном устройстве или в блокноте. В этой ситуации проблема создана не криптографией[247]. В аварии виноват чаще всего водитель, а не автомобиль.

Вирус-вымогатель из второй ситуации стал возможен благодаря криптографии, без нее такого рода программ не существовало бы, как без электричества не было бы поражений током. Польза от электричества намного превосходит опасность его повсеместного использования. Аналогичным образом я могу утверждать, что польза от шифрования существенно перевешивает проблемы от вирусов-

вымогателей. Кроме того, с этими вирусами можно бороться. Как и с любым другим вредоносным ПО, снизить риски помогает резервное копирование, поддержание системы в актуальном состоянии, установка и правильная эксплуатация антивирусных программ, а также отучение пользователей щелкать по всем подряд ссылкам и вложениям. Криптография может быть направлена против вас, но вы можете принять меры, чтобы избежать неприятностей.

Время от времени криптография может создавать трудности для сетевой безопасности. В качестве меры предосторожности в третьей ситуации можно было бы искать любые входящие данные, которые хотя бы выглядят зашифрованными, и обращаться с ними с той же степенью подозрительности, что и с любым элементом черного списка[248]. Затем можно было бы распознать допустимые случаи использования криптографии и сделать для них исключение. Но приходится признать, что защитить сеть от всех угроз, возникающих в киберпространстве, очень сложно. Даже высокозащищенные сети, не подключенные к Интернету, могут заразиться, если кто-то занесет в них вредоносное ПО вручную, например на флешке[249]. Администрирование сетей должно происходить таким образом, чтобы криптография применялась для защиты, а не для причинения вреда.

Остальные три ситуации, относящиеся к проблемным способам использования криптографии, имеют совершенно другой характер. В каждом из них фигурируют (предположительно) «плохие» люди. Но они применяют шифрование для задач того же рода, что и вы.

• Подозреваемый в убийстве зашифровал фотографии на своем телефоне точно так же, как, вероятно, делаете и вы (большинство современных телефонов шифруют все хранящиеся на них данные по умолчанию на случай, если телефон украдут).

• Растлители несовершеннолетних соединяются с сервером изображений с помощью Tor, чтобы сохранить анонимность. Для использования Tor существует множество причин, в том числе и вполне уважительных. Возможно, вы вообще не сторонник идеи неприкосновенности частной жизни и вам кажется, что любой, кто желает оставаться анонимным в киберпространстве, замышляет что-то неладное. Но что, если вы проводите журналистские расследования,

планируете стать осведомителем, работаете в органах правопорядка или просто живете в стране с деспотическим режимом?

• Предполагаемые террористы использовали систему обмена сообщениями с шифрованием, чтобы никто не мог узнать, о чем они разговаривают. Но что насчет вас? Как бы вы отнеслись к тому, что любой (не только полиция или, возможно, ваши друзья) может просматривать все ваши разговоры в Интернете? На сегодня системы обмена сообщениями все чаще применяют шифрование по умолчанию, используя самые передовые алгоритмы. Теперь приходится подсуетиться, чтобы *не* шифровать свои сообщения.

Проблема в том, что шифрование работает независимо от того, к каким данным и в каких целях оно применяется. То, чем занимаются все эти «плохие» пользователи, технически мало отличается от совершенно законных действий, которые, возможно, захочется выполнить вам. Таким образом, применение шифрования ставит перед обществом дилемму. Если общество согласно на широкое распространение криптографии, оно должно быть готово к тому, что с ее помощью будут защищаться и данные, относящиеся к незаконной деятельности. С другой стороны, если мы попытаемся каким-то образом ограничить использование шифрования, то это также помешает честным гражданам защищать свою совершенно законную личную информацию[250].

Нужно ли что-то предпринимать?

Должно ли общество пытаться контролировать распространение шифрования? На этот счет существует много разных мнений, и я подозреваю, что так будет всегда.

Довод в пользу целенаправленных действий для контроля за шифрованием страстно продвигают некоторые представители власти. В 2014 году в своем обращении к сотрудникам правоохранительных органов сэр Бернард Хоган-Хау, бывший глава Муниципальной полиции Лондона (крупнейшего полицейского подразделения в Великобритании), предостерег: «Уровень шифрования и защиты, который мы наблюдаем на устройствах и в средствах коммуникации,

затрудняют работу полиции и спецслужб по обеспечению безопасности граждан… Интернет превращается в темное и неконтролируемое пространство, где происходит обмен изображениями с признаками насилия по отношению к детям, планирование убийств и осуществление террористических атак… В демократической стране мы не можем допустить возникновение анархии в виртуальном или каком-либо другом пространстве, когда преступления происходят без страха наказания»[251].

В 2015 году Джеймс Коми, в то время директор ФБР, выразил аналогичные опасения: «По мере того как наша жизнь становится все более цифровой, логика шифрования все в большей степени состоит в том, что все, что происходит в нашей жизни, будет надежно зашифровано. Это означает, что жизнь любого человека, включая преступников, террористов и шпионов, полностью выйдет за рамки судебно-правового процесса. И это, как мне кажется, должно быть очень, очень тревожным сигналом для демократии»[252].

Американский сенатор Том Коттон использовал еще более жесткие выражения, аргументируя необходимость борьбы со свободным использованием шифрования: «Проблема сквозного шифрования относится не только к терроризму. Она также касается торговли наркотиками, похищений и детской порнографии»[253].

Однако существуют и те, кто высказывается в пользу широкого доступа к технологиям шифрования. В ответ на неоднократно звучавшие опасения о последствиях использования устойчивой криптографии Зейд Раад аль-Хуссейн, верховный комиссар ООН по правам человека, предостерег: «Шифрование и анонимность необходимы для обеспечения как свободы выражений и убеждений, так и права на неприкосновенность личной жизни. Без инструментов шифрования человеческие жизни могут оказаться под угрозой»[254].

В 1994 году, на предыдущем витке жарких дебатов об использовании шифрования, Эстер Дайсон, американская журналистка и бизнес-леди, высказала следующую мысль: «Шифрование… это мощное оборонительное оружие для свободных людей. Оно предоставляет технические гарантии конфиденциальности независимо от того, кто возглавляет правительство. …Сложно представить себе более действенный и менее опасный для свободы инструмент»[255].

Профессор компьютерных наук и криптограф Мэтт Блейз выразил мнение, которое разделяют многие исследователи: «Возможно, шифрование и в самом деле затрудняет определенные криминальные расследования. Оно может исключить использование некоторых следственных методов или усложнить получение доступа к определенным электронным уликам. Но вместе с тем оно предотвращает преступления, делая наши компьютеры, нашу инфраструктуру, наши медицинские записи, нашу финансовую информацию более защищенными от преступников. Оно предотвращает преступления»[256]. Ту же точку зрения, только лаконичнее, выразил Эдвард Сноуден: «Мы не должны относиться к шифрованию как к какой-то черной магии. Это элементарная защита»[257].

Ловим крипторыбку

Можем ли мы пользоваться защитой, которую предоставляет шифрование, но в то же время иметь возможность убирать эту защиту в определенных обстоятельствах? Иными словами, можем ли мы поймать крипторыбку, не замочив рук?

Некоторые представители власти считают, что это возможно. Этот аргумент часто приводится в пользу необходимости сбалансировать малосовместимые между собой цели. Например, безопасность обычных пользователей системы обмена сообщениями, такой как WhatsApp или Signal, должна рассматриваться с учетом того, что клиенты, пользующиеся услугами этой системы для проведения нежелательных видов деятельности, получают ту же конфиденциальность. Экс-министр внутренних дел Великобритании Эмбер Радд выступала за «балансирование шифрования и борьбы с терроризмом»[258]. Бывший директор Центра правительственной связи сэр Дэвид Оуменд отмечал, что, по его ощущениям, Великобритании удалось найти правильный баланс между (национальной) безопасностью и конфиденциальностью: «2017 – это год примирения, в котором мы, как зрелая демократия, признаем возможность

сосуществования достаточного уровня безопасности и достаточного уровня конфиденциальности»[259].

Идея существования такого баланса может показаться соблазнительной, и те, кто за нее ратуют, несомненно, имеют благие намерения. Но что это на самом деле означает? Какими единицами измерения можно пользоваться? Как узнать, достигнут ли нужный баланс? Кто это решает? И, наверное, самое важное: достижим ли такой баланс технически?

Посмотрим на этот вопрос под другим углом. Шифрование уже давно называют технологией *двойного назначения*. Этот термин отражает тот факт, что определенные технологии применяются как в гражданской, так и в военной сфере, и в целом могут использоваться как во благо, так и во вред. В этом смысле криптография находится в одной категории с радиоактивными материалами, химическими процессами, биологическими агентами, тепловизорами, камерами ночного видения, лазерами и беспилотниками – все это является для общества сложной смесью достижений и потерь. Технологии двойного назначения зачастую регламентируются разными правовыми нормами одновременно![260]

При обсуждении криптографии термин *двойное назначение* кажется мне слишком общим и скорее бесполезным. Он подразумевает, что в руках правительственных ученых эта технология безопасна, но ее попадание в руки террористов нужно предотвращать любой ценой. Это, пожалуй, справедливо для высокообогащенного плутония, но можно ли то же самое сказать о шифровании? Во времена, когда криптография была прерогативой военных, этот аргумент имел определенный вес. Но сегодня, когда она лежит в основе безопасности всех, кто находится в киберпространстве, имеет ли смысл беспокоиться о каждом, кто способен защитить свои данные с помощью устойчивого шифрования?

На мой взгляд, у криптографии больше общего с ремнем безопасности, чем с бомбой. Террорист, который едет в такси к месту совершения теракта, пристегнут так же, как и любой другой пассажир. Таким образом, ремни безопасности берегут террористов и косвенно способствуют терактам. Но вряд ли кто-то станет выступать за прекращение работы над улучшением этой меры предосторожности. Польза, которую криптография приносит множеству людей,

существенно перевешивает тот вред, который с ее помощью причиняют единицы.

В наши дни криптография используется намного шире, чем когда-либо раньше, но это отнюдь не новая технология. Споры вокруг шифрования бушуют с тех пор, как криптография стала широкодоступной[261]. Если взглянуть на отношение к этой дилемме в исторической ретроспективе, становится очевидно, что все попытки «сбалансировать» использование шифрования в лучшем случае оказывались временными мерами, которые в конечном счете были сметены технологическим прогрессом. Более того, большинство этих мер и сами приводили к проблемам[262].

Невзламываемые криптосистемы с возможностью взлома

Когда власти ратуют за возможность как-то обойти криптографическую защиту данных, полезно четко представлять себе, что они имеют в виду. В обычных обстоятельствах криптосистема должна быть достаточно безопасной для защиты информации, иными словами – невзламываемой, если говорить о практической стороне. Однако в особых случаях должны существовать средства доступа к данным, зашифрованным с помощью этой же криптосистемы, фактически механизмы, с помощью которых криптосистему можно «взломать»[263]. Вам не кажется, что такая постановка задачи изначально проблемна, поскольку противоречит сама себе? В сущности, она требует создания «невзламываемой криптосистемы с возможностью взлома».

Как вы помните, любую условную криптосистему можно взломать множеством разных способов. «Злоумышленник», роль которого в этом случае играют органы власти (объединим их в общую категорию *государство*), может проникнуть в криптосистему, пользуясь каким-то из ее аспектов: криптографическим алгоритмом, особенностями реализации, деталями процедуры управления ключами, прорехами в безопасности конечных точек. Конечно, все эти методы уже использовались в прошлом.

В большинстве обстоятельств сама идея о том, что невзламываемую систему можно взломать, прозвучала бы парадоксально. Но такую ситуацию, по крайней мере, можно себе представить, если между возможностями государства и «обычных пользователей»[264] криптосистем заложена серьезная разница. Она может касаться знаний (криптографии или архитектуры системы), вычислительных ресурсов, возможности провоцировать определенное поведение. Если государство может делать то, что никому другому не под силу, то невзламываемые криптосистемы с возможностью взлома становятся как минимум возможными.

Представьте, что государство, по всеобщему мнению, имеет такое преимущество перед всеми остальными и что существует криптосистема, которая может быть взломана за счет этого преимущества. Неважно, как это работает. Назовем пока что эту способность взламывать невзламываемое *волшебной палочкой*. Пользователи криптосистемы могут защищать свои данные с помощью шифрования, которое считается достаточно устойчивым для обеспечения конфиденциальности и защиты от любых потенциальных злоумышленников. Но как только пользователь становится фигурантом законного расследования, государство может взмахнуть волшебной палочкой, и – вуаля! – исходная информация раскрыта.

Этот пример порождает массу вопросов. Оставим в стороне спорные политические моменты и вопросы международной юрисдикции и предположим, что потребность государства в волшебной палочке никто не оспаривает. Проигнорируем заодно многочисленные процедурные и практические аспекты и поверим, что государство будет использовать эту палочку ответственно. Самый важный нерешенный вопрос, безусловно, звучит так: учитывая, что волшебная палочка существует, можем ли мы быть уверены в том, что ею не завладеет никто другой? В конце концов, даже невзламываемую систему можно *взломать*, так стоит ли верить в то, что этой возможностью взлома всегда будет пользоваться только государство? Помните об этом вопросе, пока мы с вами анализируем потенциальные волшебные палочки.

Черный ход

В качестве ориентира при рассмотрении невзламываемой криптографии с возможностью взлома можно взять Вторую мировую войну. Вплоть до ее окончания шифрование применяли только *государства*, в частности военные, которые пользовались собственными алгоритмами в собственных целях. Поскольку шифрование существовало лишь в сфере совершенно секретных коммуникаций внутри строго контролируемых организаций, соответствующие алгоритмы было логично держать в тайне. Никто другой их не использовал, и никому больше не нужно было знать, как они работают.

После войны прогресс в сфере связи спровоцировал повышение интереса к технологиям шифрования по всему миру (и снова – прежде всего со стороны правительств). Однако опыт применения криптографии был чрезвычайно ограничен, и всего несколько организаций были способны разрабатывать шифровальные устройства. Спрос на криптографию превысил предложение, сделав ее ходовым, но в то же время узкоспециализированным и деликатным товаром[265].

Теперь рассмотрим гипотетическую ситуацию, которая могла произойти, скажем, в 1950-х. Технологически развитое государство Свободия производит и продает шифровальные устройства. Свободийцы получают заказ от Руритании, отстающей в технологическом развитии, на партию шифровальных устройств для защиты руританских дипломатических коммуникаций. Свободия и Руритания не находятся в состоянии войны, но у них непростые отношения; к тому же, по мнению свободийцев, Руритании недостает политической стабильности. Должна ли Свободия продать Руритании свои новейшие разработки в области шифрования? Конечно, это возможность заработать, но в то же время это существенно затруднит свободийским спецслужбам сбор разведданных.

Обратите внимание на непропорциональные возможности этих стран. У Свободии есть знания и технологии, которых нет у Руритании. Следовательно, Свободия может внести небольшие изменения в свои невзламываемые шифровальные устройства, чтобы их можно было взломать. Иными словами, устройства и дальше будут шифровать и расшифровывать, но в арсенале Свободии появится трюк, неизвестный никому другому, который позволит ей расшифровывать данные, сгенерированные этими устройствами. Такой трюк иногда

называют *бэкдором* (англ. backdoor – черный ход), поскольку он служит средством доступа к исходной информации, о котором большинство пользователей криптосистемы ничего не знает.

Самое удобное место для устройства черного хода – собственно алгоритм шифрования. В самом примитивном варианте перед шифрованием исходных данных можно было бы сбрасывать ключ к заранее установленному значению. Руританцы бы думали, что они каждый раз используют разные ключи, как и полагается, тогда как на самом деле алгоритм всегда шифровал бы с помощью одного фиксированного значения. И это значение, разумеется, было бы известно свободийцам, что позволило бы им расшифровать руританские коммуникации.

Хочется верить, что такой бэкдор могли бы быстро обнаружить. Однако руританцы очень плохо разбираются в криптографии, поэтому они, скорее всего, даже не заподозрят, что купленные ими устройства могут работать не так, как заявлено. Но даже если какие-то подозрения возникнут, руританцам, скорее всего, не хватит знаний, чтобы разобрать эти устройства, понять принцип их работы и найти лазейку.

Как свободийцы могут вести себя настолько безнравственно! Что ж, государства обычно очень серьезно относятся к безопасности. В данном случае забота о собственной безопасности перевесила бы любые этические соображения. Важнее всего в этом примере то, что правительство Свободии уверено: его не поймают на горячем. Свободийцы и дальше будут продавать свою криптографическую продукцию по всему миру. Их решение встроить бэкдор продиктовано тем, что… они это могут[266].

Черный ход становится парадным

Существуют две очень веские причины, почему внедрение бэкдора в криптографический алгоритм как средство решения дилеммы, возникшей из-за использования шифрования, было возможно в Свободии в 1950-х, но не сегодня.

Прежде всего, в наши дни криптография играет слишком важную роль в компонентах, лежащих в основе любой криптосистемы, что исключает использование «сомнительных» криптографических

алгоритмов. Если создание невзламываемых систем с возможностью взлома действительно оправдано, то алгоритмы – не самое подходящее место для бэкдоров. Представьте, что ситуация, в которой руританскому правительству продали алгоритм шифрования с потайной лазейкой, произошла в наши дни. Свободия могла бы надеяться на то, что бэкдор позволит ей получить дипломатические разведданные, но, учитывая распространенность криптографии, тот же алгоритм мог бы применяться в руританских больницах для защиты медицинских записей. Свободийцы хотели получить преимущество в дипломатической сфере, а не ставить под угрозу безопасность личных конфиденциальных данных всего населения Руритании.

Вторая причина, наверное, более фундаментальна. Свободийцам, может, и сошло бы с рук внедрение бэкдора в алгоритм в 1950-х, но не сегодня. Мы уже знаем намного больше о криптографии и разработке криптографических алгоритмов, чем раньше, и в мире хватает специалистов, способных эти алгоритмы проанализировать. Современные реалии таковы, что публикация, исследование и одобрение криптографических алгоритмов для общественного использования – действия само собой разумеющиеся[267]. Даже когда алгоритмы поставляются вместе с аппаратным обеспечением, их можно проанализировать и проверить. При обнаружении бэкдора специалисты забьют тревогу, и никто не станет применять такой алгоритм. С другой стороны, любой, кто уже пользуется этим алгоритмом, окажется в опасности.

Наверное, самым известным примером криптографического алгоритма двадцать первого века, в который попытались внедрить бэкдор, был *Dual_EC_DRBG*. Этот алгоритм предназначался не для шифрования, а для генерации псевдослучайных чисел и создания криптографических ключей. Представители Агентства национальной безопасности США (АНБ) поспособствовали его принятию в качестве международного стандарта, но криптографы быстро почуяли неладное[268]. Мы не один раз уже говорили, что существуют средства и способы предугадать вывод этого генератора. Конечно, в результате ключи, которые он генерировал, были предсказуемы, что, в свою очередь, позволяло расшифровать зашифрованные с их помощью данные. В итоге после громкого скандала Dual_EC_DRBG убрали из списка стандартов[269].

Внедрение бэкдора в современный криптографический алгоритм было бы безрассудным поступком с высоким риском возникновения непредвиденных и нежелательных последствий. Дисбаланса в знаниях о криптографии, который существовал в 1950-х, давно уже нет. В наши дни любой черный ход легко становится парадным[270], делая бессмысленным использование шифрования как такового.

Вытягиваем длинную руку закона

Есть одна область, в которой государство неизменно сохраняет преимущество перед всеми остальными. Да, разумеется, речь идет о способности создавать правовые нормы и обеспечивать их соблюдение. Для борьбы с «проблемами», которые создает криптография, ее использование можно регламентировать.

Посмотрим на еще один пример. Давным-давно существовала технология, которая помогала людям обмениваться идеями по-новому. Очень скоро она попала в поле зрения властей, которые сделали обязательным ее лицензирование и ввели контроль за ее импортом и экспортом. Некоторые государства ее попросту запретили. Последующий период характеризуется попытками преодолеть эти ограничения. Государства мотивировали необходимость контроля за технологией соблюдением правопорядка. Пользователи и поставщики этой технологии призывали отменить эти правовые нормы во имя политической свободы и прав человека.

Это была история о печатном станке, который был изобретен в середине пятнадцатого века и больше трехсот лет служил политическим яблоком раздора[271]. В конечном счете общественное давление в сочетании с технологическим развитием привело к ослаблению контроля за книгопечатанием в большинстве стран мира (хотя в некоторых странах, например, в Японии, эта либерализация произошла относительно недавно). Однако ту же историю, слово в слово, можно было бы рассказать и о судьбе криптографии после Второй мировой войны.

Самой неуклюжей правовой реакцией на появление любой, даже нежелательной, технологии является ее полный запрет. Некоторые

страны, такие как Россия и Османская империя, настолько сильно опасались распространения идей в книгах, что попытались запретить печатный станок[272]. В наши дни некоторые государства, к примеру, Марокко и Пакистан, делают нечто похожее, объявляя вне закона использование и продажу технологий шифрования без предварительного одобрения правительства.

Обосновать современные запреты на шифрование, а уж тем более обеспечить их соблюдение, крайне сложно. Криптография слишком широко распространена и приносит слишком много пользы для того, чтобы в самом деле с ней бороться.

Более распространенный подход к контролю за технологиями шифрования состоит в ограничении их импорта и экспорта, как это происходило с печатным станком. Это самый логичный выход из ситуации в мире с ограниченным кругом поставщиков таких технологий. Но этого мира давно нет. Импортер, такой как Руритания, может самостоятельно решать, какие средства шифрования попадают в страну. Экспортер, такой как Свободия, может решать, кому продавать свою продукцию. Экспортные ограничения позволяют государству определить степень устойчивости алгоритмов шифрования, которые позволено ввозить или вывозить из страны. В начале 1990-х печально известный закон США не позволял экспортировать технологии симметричного шифрования с ключами, длиннее 40 бит. Можно смело предположить, что в АНБ считали осуществимым поиск ключей этой длины методом полного перебора. Например, веб-браузер Netscape поначалу имел две версии: американскую, которая поддерживала устойчивое 128-битное шифрование, и международную экспортную версию с 40-битной защитой. Хотя нельзя сказать, чтобы этот подход не вызывал споры[273].

Экспортные и импортные ограничения и в самом деле можно назвать действенным средством контроля за распространением материальных объектов, которые можно проинспектировать на границе. Вплоть до 1970-х годов шифрование выполнялось при помощи крупных тяжелых устройств, которые было сложно даже сдвинуть с места. Таким образом ограничения на перемещение средств шифрования могли соблюдаться хотя бы на границе (по крайней мере, теоретически).

Ситуация радикально поменялась к концу двадцатого века, когда шифрование в программном обеспечении стало более доступным. Перемещение такого ПО по всему миру почти невозможно контролировать, так как это, в сущности, всего лишь набор инструкций, которые выполняет компьютер. В знак протеста против экспортных ограничений США исходный код средств шифрования RSA был задокументирован в книге и даже напечатан на футболках, что мгновенно превратило их из невинных предметов одежды в незаконное военное снаряжение, запрещенное к вывозу[274]. В наши дни программное обеспечение перемещается по миру одним щелчком мыши или нажатием клавиши.

Обеспокоенность государства использованием криптографии, выраженная в импортных и экспортных ограничениях, постепенно ослабла, и это, конечно, тоже начало приводить к нелепым ситуациям. В конце 1990-х я участвовал в многостороннем европейском проекте по разработке программной системы, которая должна была продемонстрировать применение криптографии в микроплатежах с помощью мобильных телефонов. Эта система работала на стандартном персональном компьютере и была реализована одним из партнеров из южной части Германии. Европейская комиссия потребовала, чтобы этот проект был показан на мероприятии в Комо на севере Италии. Для немцев это могло бы стать простой четырехчасовой поездкой через Швейцарию, однако швейцарские законы относительно экспорта криптографии требовали особую лицензию для провоза такого ПО через их границу. В итоге моим немецким коллегам пришлось сделать грандиозный, хотя и довольно живописный двенадцатичасовой крюк по австрийским Альпам, чтобы не пересекать границу Швейцарии. Столько времени и энергии ушло впустую, и все из-за довольно архаичного решения «проблемы» криптографии!

Путь к Криптопии

1990-е прошли в неуклюжих попытках государств найти баланс между национальной безопасностью и конфиденциальностью. Экспортные ограничения хорошо справлялись со своей задачей, но

ситуация менялась. Проблема была не в том, что устойчивая криптография, включая асимметричное шифрование, стала частью общественной жизни, эти знания были доступны уже на протяжении двух десятилетий. Радикальное изменение, произошедшее в 1990-х, состояло в том, что люди наконец обратили на это внимание.

Прогресс в области компьютеров и сетей, которые их соединяют, привел к возникновению двух совершенно разных взглядов на то, как взаимосвязанные устройства повлияют на наше будущее. Одни просто распознали новые коммерческие возможности. Другие же мечтали о новом обществе, свободном от оков традиционной государственной власти.

Правительства, намеревавшиеся сохранить контроль за шифрованием, могли бы, наверное, договориться с предпринимателями новой волны. Куда сложнее было противостоять социальным изменениям. Свежесозданный Интернет, зарождающаяся Всемирная паутина, показали многим совершенно новый мир, в котором можно было творить потрясающие вещи: незнакомые единомышленники со всего мира могли обмениваться идеями; можно было торговать глобально без оплаты через кассу; люди, у которых не было возможности встретиться лично, могли формировать виртуальные сообщества.

Существовали и более радикальные представления. Некоторые энтузиасты осознали, что эти новые виды деятельности могут не подчиняться общепринятым социальным ограничениям. В киберпространстве можно было устанавливать новые, «народные» правила. Это не было анархией в традиционном понимании, так как никто не ставил целью избавление от органов государственной власти. Киберпространство должно было стать параллельной реальностью, в рамках которой можно было обойти некоторые нормы, сложившиеся в государстве.

Все эти видения принципиально опирались на идею о том, что в этом новом киберпространстве можно будет хранить секреты. Эти будущие миры нуждались в шифровании – и не просто ради конфиденциальности, но и для того, чтобы сделать возможной анонимность. Криптография внезапно стала знаменем, вокруг которого сплотились сторонники этих идей. Такие объединения, как *киберпанки* и *криптоанархисты*, публиковали манифесты, в которых

подчеркивалась важность криптографии для построения нового общества[275]. В «Манифесте Криптоанархизма» Тимоти Мэй назвал асимметричное шифрование (предположительно, имея в виду RSA) «незначительным, казалось бы, открытием из загадочного раздела математики», которое «снимет колючую проволоку с интеллектуальной собственности»[276]. Звучит сильно!

Утопические взгляды на то, как криптография могла бы изменить мир, в какой-то степени объяснялись глубоким недоверием к государству. Однако опасения по поводу контроля за криптографией высказывали далеко не только радикалы. Многие инженеры понимали, насколько важной станет криптография в будущем, и опасались, что ограничения со стороны правительств навредят развитию кибербезопасности.

Правительства занервничали, и не без оснований. Широкий доступ к технологиям шифрования и анонимности ставил под угрозу эффективность нескольких аспектов сложившейся модели государственного управления, включая сбор разведданных и борьбу с преступностью. Ограничения на вывоз средств шифрования все больше напоминали слабую плотину на грани прорыва, и сторонники менее ограниченного доступа к криптографии уже могли видеть, как на ней образовываются трещины. Необычный союз вольнодумцев, инженеров, корпораций и борцов за гражданские права начал громко требовать ослабления контроля за криптографией. Они выпускали свободное криптографическое ПО – в частности, PGP[277] (Pretty Good Privacy) Филиппа Циммерманна. Они инициировали судебные иски, такие как *Бернштейн против Соединенных Штатов*[278]. Они даже объявили войну.

Криптовойна

В 1990-х началась так называемая *криптовойна*, которая продолжается по сей день (некоторые утверждают, что она намного древнее). Конечно, война – это слишком сильно сказано, поскольку до стрельбы пока не дошло, однако вокруг контроля за криптографией

идут жаркие споры, которые время от времени преподносятся как вопрос жизни и смерти.

Эпицентром криптовойны была и остается Америка, хотя конфликт сам по себе глобальный. Многие приписывают ее начало администрации Билла Клинтона, который хотел контролировать использование криптографии в период стремительных технологических изменений. Основная идея была далека от утонченности и звучала так: «Вам нужна криптография? Пользуйтесь сколько влезет и для чего угодно; только не забудьте поделиться с нами ключом для расшифровки». Ого! Да неужели?

Согласно этому плану, который официально назывался *депонирование ключей*, тот, кто хотел что-то зашифровать, должен был использовать одобренные алгоритмы и передать ключ для расшифровки правительству. Этот ключ, по крайней мере формально, был доступен только государству и мог применяться только на основании постановления суда.

Можете себе представить, как общество встретило идею депонирования ключей в качестве средства контроля за криптографией! Выражались сомнения в безопасности: можно ли доверить государству хранение ключей расшифровки? Обсуждались материально-технические вопросы: как системы депонирования ключей будут разрабатываться и интегрироваться в бизнес-процессы? Была озабоченность финансовым аспектом: кто за все это будет платить?[279] Но самый важный вопрос звучал так: какую проблему на самом деле решало депонирование ключей?

Если конечной целью было открыть государству доступ к данным, которые зашифрованы фигурантами расследований, какой смысл был такому фигуранту вообще пользоваться депонированной криптосистемой? В 1990-х программное обеспечение для шифрования уже было общедоступным, и любой, кто хотел скрыть свою информацию, мог сделать это без алгоритмов, одобренных правительством, и без передачи ключа. Становилось ли применение недепонированного шифрования преступлением? Как поговаривали киберпанки, «если шифрование вне закона, им будут пользоваться только преступники»[280].

Депонирование ключей не прижилось. Экспортные ограничения на криптографию пришлось ослабить. С началом нового века мы вошли в

эпоху явного прагматизма по отношению к контролю за криптографией. Такие страны, как Великобритания, понимая свою неспособность лицензировать или депонировать средства шифрования, приняли законы, согласно которым подозреваемые, обладающие зашифрованными данными, обязаны выдать ключи для расшифровки по решению суда.

С точки зрения государства, впрочем, это довольно громоздкий подход. Во-первых, нужно соблюсти юридические формальности. Во-вторых, подозреваемого нужно убедить в необходимости сотрудничества. И наконец, подозреваемый должен найти свой ключ и передать его следствию, хотя ничто не мешает «забыть» его или «потерять» (не говоря уже о риске, что он и вправду не имеет ни малейшего понятия, где его ключ находится)[281].

Тем временем масштабы использования криптографии стремительно росли. Средства шифрования распространились максимально широко. Криптография стала частью повседневных технологий. Устройства с устойчивым шифрованием начали продавать в большинстве стран без правовых ограничений.

Однажды, вскоре после того, как угасла инициатива по депонированию ключей, я сидел в офисе одного мудрого коллеги, пионера в области криптографии. «Больше нет пути назад, правда? – заметил я. – Криптография вышла из-под контроля, и уже никому нельзя запретить ею пользоваться. Мы выиграли криптовойну». Это было распространенное мнение среди тех, кто следил за ситуацией вокруг депонирования ключей. Мой коллега откинулся на спинку кресла, усмехаясь моему простодушию: «Все еще впереди, вот увидишь».

То, что он понимал тогда, теперь известно всем. Криптовойна продолжается, и у нее никогда не будет победителя.

Эпоха массового шифрования

За первое десятилетие двадцать первого века в криптовойне произошло всего несколько публичных схваток. И вовсе не потому, что война подошла к концу. Просто одна из сторон конфликта была занята экспериментами со всей той криптографией, за освобождение которой

от государственного контроля она так страстно сражалась. А враг тем временем не дремал.

В эпоху общедоступной информации и массового применения криптографии, когда любой может изобрести и использовать собственный устойчивый алгоритм шифрования, может показаться, что государство больше не обладает преимуществом в этой сфере. Правительственные организации действительно утратили явное лидерство в области криптографических алгоритмов. По всей видимости, превосходства с точки зрения вычислительных ресурсов у них тоже нет, поскольку даже самому мощному суперкомпьютеру в мире не по зубам шифрование AES.

Однако у государства по-прежнему есть несколько важных козырей. Один из них состоит в том, что государство обычно контролирует ключевую физическую инфраструктуру, такую как магистральные сети, от которых зависит киберпространство. Еще одним козырем государства является возможность регламентировать работу организаций, продукция и услуги которых позволяют нам взаимодействовать с киберпространством; это касается, к примеру, интернет-провайдеров. Разумеется, у государства по-прежнему есть обширные вычислительные и человеческие ресурсы, которые могут быть направлены на решение «проблемы криптографии». Но, наверное, самое важное преимущество государства заключается в его уникальной способности видеть общую картину того, как данные перемещаются по сетям, пронизывающим киберпространство, и где они оседают.

Часто можно услышать, что *сложность – враг безопасности*[282]. Мы создали невероятно сложное киберпространство и продолжаем его развивать. Для защиты нашей деятельности в нем существует множество замысловатых криптографических средств. Криптография должна быть тщательно реализована и интегрирована. Ключи должны храниться в надежном месте. Приходится уделять внимание тому, где оседают незащищенные данные до шифрования и после расшифровки. Помните, что криптосистему можно взломать многими способами, и в наши дни лишь некоторые имеют отношение к взлому криптографических алгоритмов.

В полной мере криптовойна возобновилась в 2013 году. Как и некоторые другие особенно грязные конфликты в истории, это было

спровоцировано попыткой покушения.

Маски сброшены

При обсуждении Эдварда Сноудена необходимо разделять этические аспекты его поступка и то, что он раскрыл. Сноуден, контрактник АНБ, опубликовал огромный массив конфиденциальной информации, включая методы, с помощью которых АНБ боролось с проблемами, возникающими из-за шифрования в ходе разведывательной работы. Это была сокрушительная череда утечек, которые пролили свет на многие инструменты, методики и тактические приемы из арсенала АНБ. Сноудену пришлось покинуть страну[283].

Вопрос, заслуживает Сноуден памятника или места за решеткой, мы обсудим в другой раз (или в другой книге). Неоспоримым остается факт, что у нас теперь есть представление о том, как некоторые страны (в частности, США и Великобритания) отреагировали на невозможность реализовать депонирование ключей. Государство могло бороться с использованием криптографии множеством способов. Благодаря Эдварду Сноудену мы можем быть уверены, что *все* они пошли в ход.

Конечно, *все подробности* происходящего нам узнать неоткуда. Сноуден опубликовал внушительную подборку документов и докладов[284], но большинство из них недостаточно детальны, и их достоверность сложно подтвердить. Однако общая картина ясна: государство, не желая отказываться от разведывательных целей, делало все возможное, пытаясь победить криптографию.

Останавливаться на конкретных обвинениях, которые могут быть обоснованными, а могут и не быть – бесплодная тактика. Мы рассмотрим широкий спектр того, что государство *могло бы* сделать. Это будет более информативно. Давайте представим себе вещи, которые государству вполне по силам, особенно если у него есть влияние на некоторые из самых могущественных технологических компаний. Часть из приведенных ниже методик упоминаются в разоблачениях Сноудена.

• Государство со значительными финансовыми ресурсами, охватом и оборудованием может хранить как можно больше данных, проходящих по киберпространству, в том числе и зашифрованных. Это могут быть копии всех данных, которые проходят через крупный центр входа в национальную компьютерную сеть (в Великобритании, к примеру, существенная часть данных приходит по подводным кабелям, которые достигают суши в нескольких удаленных местах). Государство может проанализировать эти данные и сформировать исчерпывающую картину деятельности отдельно взятого человека в киберпространстве. Даже если все его сообщения и телефонные звонки зашифрованы, привязывание сведений о том, кто с кем (и когда) общался, к такой информации как история посещения веб-страниц, может дать подробное представление о жизни подозреваемого.

• Государство может договориться с компанией, предоставляющей доступ в Интернет и услуги электронной почты миллионам граждан. Скорее всего, эта компания использует шифрование для защиты электронных писем своих клиентов и соединений с серверами, где эти письма хранятся. Она может дать государству доступ ко всем метаданным, связанным с деятельностью своих пользователей, расшифровать переписку именем государства или выдать органам власти необходимые ключи для расшифровки.

• Государство может нанять специалистов по кибербезопасности, чтобы те взломали сеть компании и тайно заполучили данные, например, перехватывая незашифрованный трафик в незащищенных внутренних сетях.

• Государство может заменить открытый ключ предполагаемого получателя, с помощью которого сетевой коммутатор шифрует трафик, своим собственным. Затем государство может расшифровать трафик, используя свой закрытый ключ, скопировать исходные данные и заново их зашифровать с помощью правильного открытого ключа. Получателю придет правильно зашифрованный трафик, и он ни о чем не догадается.

• Государство может повлиять на процессы стандартизации шифрования, чтобы для широкого применения был одобрен криптографический алгоритм с бэкдором.

• Государство может разработать или купить средства для осуществления кибератак, которые еще не получили широкую

известность, и от которых, следовательно, еще нет защиты (их иногда называют *эксплойтами нулевого дня*). Государство может вынудить подозреваемого, использующего криптографию, щелкнуть по ссылке или открыть вложение, которое инициирует атаку на его смартфон. В результате такой атаки, к примеру, можно прочитать данные еще до того, как они будут зашифрованы, похитить ключи для расшифровки или включить микрофон смартфона, чтобы записывать зашифрованные звонки[285].

Откровенно говоря, сведения, раскрытые Сноуденом, оставляют не так много пространства для фантазии.

Жизнь после Сноудена

Стал ли мир безопасней в результате разоблачения, сделанного Сноуденом, – вопрос субъективный. Майкл Хайден, бывший директор АНБ, назвал поступок Сноудена «крупнейшей утечкой реальных американских тайн в истории страны»[286]. С чисто разведывательной точки зрения Хайден вполне может быть прав, но я бы отметил, что с точки зрения нашей безопасности в киберпространстве мы, возможно, только выиграли, поскольку общество в целом теперь лучше понимает соответствующие проблемы и имеет возможность их обсуждать.

Наверное, самое важное – то, что это разоблачение послужило эффектным и своевременным напоминанием о том, насколько уязвимо киберпространство. Интернет – это не тщательно спроектированная сеть со встроенными средствами безопасности. Киберпространство, с которым мы имеем дело, эволюционировало в хаотичной и несогласованной манере, а безопасность почти всегда обеспечивалась с запозданием (а то и вообще отсутствовала). В целом киберпространство полно дыр в безопасности, вызванных слабыми местами в технологиях, плохой интеграцией разных систем, несоблюдением процедур и неэффективным управлением. Даже когда мы шифруем данные, эти дыры оставляют массу возможностей для тех, кто пытается что-то узнать. Но, как это часто бывает со скрытой

истиной, пока не прольется свет на реальное положение дел, мы не спешим делать даже то, что необходимо сделать[287].

Информация, раскрытая Сноуденом, имеет далеко идущие последствия. В контексте криптографии самым серьезным из них можно назвать распространение *сквозного* шифрования среди множества поставщиков технологий, таких как компания Apple, которая использует его в своей системе обмена сообщениями. У любого шифрования есть начальная и конечная точки. Сквозным оно становится в случае, когда этими точками выступают устройства, находящиеся под контролем сторон взаимодействия, а не сервера между ними. Помимо прочего, это должно означать, что поставщик услуги (такой как компания Apple с ее системой обмена сообщениями) не в состоянии расшифровать это взаимодействие.

К большому недовольству некоторых государственных органов, сквозное шифрование исключает некоторые методы получения исходных данных, в том числе и сотрудничество с корпоративным поставщиком услуги (добровольное или принудительное). В 2016 году в ходе судебных разбирательств между Apple и ФБР вокруг доступа к зашифрованному iPhone, сторонники правоохранительных органов утверждали, что руководство компании отдало предпочтение «защите личных данных мертвого террориста ИГИЛ[288] перед безопасностью американских граждан»[289], а глава Apple Тим Кук заявил, что согласиться с требованиями ФБР было бы подобно созданию «программного эквивалента ракового заболевания»[290].

На более фундаментальном уровне эти разоблачения привели как минимум к общественному обсуждению проблемы шифрования и его влияния на работу госслужб. Комментируя трудности доступа к зашифрованным данным, бывший премьер-министр Австралии Малкольм Тернбулл довольно смело заявил, что «законы математики – это хорошо, но в Австралии действуют только австралийские законы»[291].

Сам факт того, что столько видных деятелей выразило свое мнение насчет шифрования, будь то в пользу или против контроля за его применением, можно считать хорошим признаком. Некоторые страны, включая Австралию, Великобританию и США, занялись пересмотром соответствующего законодательства. Многие пользователи узнали о технологиях шифрования, что породило спрос на их внедрение в

различные сервисы. Сеть Tor выросла более чем в четыре раза по сравнению с 2010 годом[292]. Многие влиятельные компании отреагировали на происходящее, улучшив свою криптографическую безопасность[293].

Время покажет, приведет ли поступок Сноудена к существенным изменениям в реализации и использовании криптографии. В любом случае он дал обществу достаточно пищи для размышлений о том, как мы генерируем данные, как за этими данными следят государственные структуры, и о дилемме, которую порождает применение шифрования. Само по себе обсуждение этих проблем ничего не решает, но было бы куда хуже, если бы мы о них так и не знали.

Реальная криптополитика

В каком-то смысле победителями в криптовойне можно считать сторонников неограниченного использования криптографии. Сегодня все мы используем устойчивое шифрование, и нет пути назад к эпохе, в которой государства могли определять степень устойчивости криптографических алгоритмов и их назначение. Многие правительства открыто признали, что криптография играет ключевую роль в формировании безопасного цифрового общества[294].

Тем не менее мечты о том, что криптография станет базовой технологией для создания нового мира, остаются мечтами. Криптография серьезно препятствует государствам, которые (наверное, обоснованно) пытаются с этим бороться. Бэкдоры в криптографических алгоритмах и ограничения на вывоз криптографических устройств больше не считаются подходящими рычагами для решения упоминавшейся дилеммы. Однако похоже, что некоторые из «невзламываемых» криптосистем, которыми мы пользуемся на сегодняшний день, *слишком* уж легко взломать. Киберпространство очень сложное, и у него слишком много потенциально слабых мест, которые могут служить не только государственным властям, пытающимся получить доступ к исходным данным, но и разного рода злоумышленникам. Распространение криптографии, не предусматривающей государственного контроля,

заставило правительства перенять не вполне традиционные методы борьбы с шифрованием, которые иногда оказываются непропорциональными и могут подвергать наши компьютерные системы риску[295].

Я уверен, вы надеетесь, что этот спор когда-нибудь завершится на оптимистичной ноте. Возможно, существует проект мирного соглашения между участниками криптовойны? Мне бы и самому хотелось предложить элегантный выход из этой ситуации, но у меня нет готового решения, и оно вряд ли есть у кого-то другого. Тем не менее я могу высказать некоторые мысли о том, как может выглядеть наше будущее, но это, конечно, нельзя назвать планом полного прекращения криптобоевых действий.

Пожалуй, самое большое препятствие на пути к прекращению криптовойны – поведение и сущность сторон конфликта. Диалог происходит на повышенных тонах (когда происходит) и содержит много неопределенностей; пожалуй, никто не хочет признавать вполне обоснованную озабоченность своих оппонентов касательно настоящего и будущего криптографии. Такая неуступчивость опасна. Бывший Президент США Барак Обама при рассмотрении потенциальных нормативных изменений отметил: «Если все разойдутся по своим углам, и технологическое сообщество скажет: „либо давайте нам идеально устойчивое шифрование, либо это Большой брат, и мы живем в мире Оруэлла“, мы придем к тому, что в случае какого-то ужасного бедствия политический маятник качнется в другую сторону, и начнут звучать небрежные и поспешные требования, которые пройдут через Конгресс и возымеют опасные и плохо продуманные последствия»[296]. Это примерно то, где мы с вами сейчас находимся.

Чтобы бороться с нехваткой взаимопонимания, необходимо укреплять взаимное доверие и постоянно поддерживать максимально четкий диалог. В случае с криптографией проблема обычно заключается в том, что одна из двух сторон, разведывательные ведомства, традиционно находится в тени и не стремится к прозрачности. Если мы хотим добиться реального прогресса, это препятствие необходимо преодолеть хотя бы частично.

Еще одна причина, почему мы находимся в таком затруднительном положении в отношении шифрования, состоит в том, что архитектура

киберпространства, и в частности Интернета, представляет собой полнейший бардак. Эта беспорядочность плохо влияет на безопасность и дает возможность воспользоваться слабыми местами криптографической инфраструктуры. Более аккуратная и прозрачная архитектура была бы предпочтительнее, но такие вещи не так просто модернизировать. Если бы в переработанной архитектуре были предусмотрены какие-то механизмы для законного доступа к исходным данным, то можно было бы, по крайней мере, надеяться на понимание, обсуждение и принятие сопутствующих рисков[297]. Теоретически.

Так же стремительно растет и доля технологий и сервисов под контролем всего нескольких государств. Разве кого-то удивит, что США, где родились Интернет и большинство влиятельных компаний в киберпространстве, пользуется этим преимуществом, когда шифрование мешает решению других задач? Появится ли когда-нибудь возможность создать более справедливое и демократическое в геополитическом смысле киберпространство?

Мы вполне резонно применяем криптографию, чтобы защитить себя в виртуальном мире. Я не говорю, что мы должны это прекращать, я лишь указываю на то, что иногда использование криптографии может оказаться *чрезмерным*.

Задумайтесь на секунду о мобильных телефонах. Ваши звонки шифруются на отрезке между вашим телефоном и ближайшей базовой станцией; таким образом, ваш разговор нельзя перехватить с помощью простого радиоприемника. После этого данные, как правило, расшифровываются и поступают в стандартную телефонную сеть. Повторное шифрование происходит только перед тем, как данные отправляются от базовой станции к получателю с мобильным телефоном. Иными словами, звонок не зашифрован на большей части своего маршрута. Это и не требуется, поскольку проникнуть в стандартную телефонную сеть относительно непросто[298]. Государство никогда не сетует на то, что мы пользуемся сотовой связью, поскольку в случае реальной необходимости государство может перехватывать телефонные разговоры после их расшифровки (соблюдая все правовые процедуры). С другой стороны, люди редко жалуются на то, что у государства есть такая возможность. Похоже, мы

в основном не против ее использования органами власти и лишь надеемся, что они это делают ответственно?

Теперь представьте, что вы отправляете сообщение со своего мобильника, пользуясь безопасным приложением. Если это приложение поддерживает сквозное шифрование, ваше сообщение будет зашифровано на всем отрезке путешествия от одного телефона к другому. Это более надежная защита конфиденциальности по сравнению с той, которую вы получаете при выполнении телефонных звонков и отправке электронных (или даже бумажных) писем. С одной стороны, это замечательно. Но *действительно* ли необходим такой уровень конфиденциальности? Если бы мы вели переговоры об установлении новых взаимоотношений между государством и человеком в контексте криптографии, согласились бы пользователи шифрования сделать некоторые уступки в отношении того уровня криптографической безопасности, которым мы наслаждаемся сегодня? [299]

У ограничения использования криптографии уже есть прецедент. Во время холодной войны в рамках второго раунда переговоров об ограничении стратегических вооружений (ОСВ-II) Соединенные Штаты и Советский Союз согласились не применять шифрование при тестировании определенных видов оружия, чтобы другая сторона могла собирать разведданные об их назначении и возможностях[300]. В этом случае ослабление криптографии могло показаться шагом назад, если говорить о защите информации, но на деле оно помогло снизить напряжение, так как обе стороны могли узнать о возможностях друг друга. Обмен сообщениями по телефону и тестирование вооружений – это, несомненно, совершенно разные вещи, но суть в том, что иногда ослабление безопасности может быть оправданным.

Поймите меня правильно, я обеими руками за сквозное шифрование. Киберпространство остается хаотичным местом, государства продолжают перехватывать всю информацию подряд, а компании, предоставляющие инфраструктуру, обращаются с пользовательскими данными отнюдь не самым прозрачным образом, поэтому сквозное шифрование кажется самым безопасным механизмом, предлагающим адекватную защиту передаваемых данных. Я лишь пытаюсь показать, что в киберпространстве будущего у нас может появиться возможность

по-новому взглянуть на то, что же следует считать крайне необходимым.

Один из путей, который кажется ближе к переосмыслению криптографической дилеммы, нежели к полноценному решению, состоит в размежевании киберпространства. Некоторые «подпространства» могут быть более «безопасными», чем остальные. Люди могли бы присоединяться к этим виртуальным закрытым сообществам, получая тем самым определенный уровень защиты. Если архитектура этих безопасных пространств и методы управления ими будут пользоваться достаточным доверием, люди могут согласиться на то, чтобы у государства был какой-то доступ к их внутреннему зашифрованному трафику, главное, чтобы этот доступ происходил открыто и в рамках закона. За пределами этого безопасного оазиса, в менее благополучных местах, продолжит бушевать криптовойна.

Идея такого размежевания на самом деле уже постепенно воплощается в жизнь. Компания Apple, к примеру, создала ограниченное пространство для пользователей своих устройств, где можно устанавливать только определенное одобренное программное обеспечение. Некоторые люди критикуют Apple за слишком жесткий контроль, а другие с готовностью пользуются ее технологиями, уверенные, что это дает им большую безопасность.

Но ограничение загрузки ПО – это одно, а предоставление доступа к зашифрованному трафику – совсем другое. Реально ли в принципе спроектировать систему, в которой такой доступ гарантированно остается под контролем соответствующих властей? Ответ на этот вопрос далеко не очевиден. И конечно же, большинство людей, чьими действиями государство на самом деле обеспокоено, никогда не станут использовать такую систему.

Прекращение криптовойны возможно только в случае, если мы начнем тщательное и конструктивное обсуждение того самого киберпространства будущего, в котором мы бы хотели находиться. Дэниел Мур и Томас Рид предлагают следующий аргумент:

В будущем проектирование криптосистем должно определяться прагматичными политиками и техническими соображениями. Необходима принципиальная, но реалистичная оценка шифрования и технологий в целом, опирающаяся на проверенные факты и реальное

поведение пользователей, которая является результатом трезвой государственной политики, а не деятельности киберпанковых культов, верящих в технологическую чистоту и мечтающих о рукотворных утопиях. Прагматизм в принятии политических решений уже давно называется реальной политикой. Политика в сфере технологий слишком часто становится исключением. Пришло время реальной криптополитики[301].

Киберпространство, бесспорно, таит в себе опасность, но мы в основном с ней справляемся, приняв некоторые меры предосторожности. Даже те из нас, кто знает о потенциальном наблюдении со стороны государства, просто жмут **Ввод** и продолжают заниматься своими делами. Но мне кажется, что тем, кто решает воспользоваться криптографией, будет полезно знать, какой уровень безопасности они получают, чтобы не гадать, что на самом деле происходит. Мы должны смириться с тем, что использование криптографии создает дилемму, но реакция государства на нее должна быть прозрачной и приемлемой для нас. Мечтать не вредно.

9. Наше криптографическое будущее

Сегодня в нашем распоряжении есть замечательные криптографические инструменты для защиты многого из того, чем мы занимаемся в киберпространстве. Конечно, использование шифрования порождает социальные дилеммы, но они не в состоянии сдержать дальнейшее распространение криптографии, так как она слишком полезна. Криптография никуда не денется. Но каким будет ее будущее?

Будущее уже наступило

Представьте, что у вас есть письмо, содержимое которого должно оставаться конфиденциальным даже в отдаленном будущем. Вы храните его в сейфе с самым современным замком и спокойно себе спите, пока однажды, спустя десятилетие, вам на глаза не попадается заметка в газете о том, что воры научились взламывать сейфы этой модели. В ответ вы покупаете новый сейф с еще более надежным замочным механизмом и кладете свое письмо туда. Еще через несколько лет ситуация повторяется, и вы покупаете еще один сейф и т. д. Иными словами, совершенствуются не только методы взлома сейфов, но и ваша защита от них.

Для сейфов эта стратегия подходит хорошо, но с шифрованием процесс немного иной. У вас есть конфиденциальное письмо. Вы создаете множество его копий и помещаете каждую из них в отдельный сейф с самым современным замком. Вы раздаете все эти сейфы своим злейшим врагам. Десять лет спустя вы узнаете, что сейфы этой модели могут быть взломаны, поэтому вы покупаете целую кучу новых сейфов и просите своих врагов вернуть старые сейфы, чтобы вы могли их заменить[302]. Хм, ничем хорошим это не закончится, не так ли?

Проблема в том, что цифровую информацию крайне просто копировать и хранить. Нам имеет смысл исходить из того, что зашифрованные данные всегда доступны злоумышленнику. Учитывая

возможные будущие прорывы в сфере криптографических атак, полагаться на обновление алгоритма шифрования для защиты существующих данных нет смысла. Вы можете заново зашифровать тот же исходный текст с помощью новых, более надежных средств шифрования, но вы не можете гарантировать, что копии прежнего шифротекста не останутся доступными злоумышленнику, желающему их взломать[303].

Самый серьезный вызов, стоящий перед разработчиками криптографических алгоритмов, состоит в том, что сегодняшняя криптография *будет* проверена на прочность в будущем. Если уже используемый алгоритм окажется небезопасным, время и деньги, необходимые для его замены, могут быть существенными[304]. Когда в 1990-х под сомнение была поставлена безопасность блочного шифра DES, он уже был настолько глубоко интегрирован в банковскую инфраструктуру, что избавиться от него оказалось практически невозможно. В итоге мы до сих пор используем эту технологию, хоть и в более защищенном варианте, Triple DES.

В связи с этим современные криптографические алгоритмы разрабатываются в очень консервативном ключе, с жесткими требованиями к безопасности и как можно большим заделом на будущее. Разработчики пытаются предвидеть будущее развитие компьютеров, особенно в отношении вычислительных ресурсов, с существенной поправкой на ошибку. Как вы помните, самый быстрый на сегодня компьютер будет искать 128-битный ключ AES на протяжении 50 миллионов миллиардов лет. Такая защита может показаться излишней, но мы хотим шифровать данные так, чтобы они оставались конфиденциальными даже через двадцать пять лет (а в некоторых случаях и намного дольше). Насколько мощным будет самый быстрый компьютер к тому времени? Осторожный подход к проектированию AES предусматривает более длинные, 192- и 256-битные ключи, которые можно использовать уже сегодня для данных, требующих чрезвычайно высокого уровня защиты, или перейти на них в будущем, чтобы сэкономить.

В контексте криптографии будущее должно заботить нас уже сегодня. Неважно, как именно оно будет выглядеть, главное, что мы к нему готовимся.

Кванты

Слово *квантовый* оказывает на людей чуть ли не гипнотический эффект. Оно вызывает в воображении увлекательные и иногда тревожные образы сложных технологий будущего, которые мы даже не можем себе представить[305]. Мы ошеломленно качаем головой и думаем: «Лучше оставить это специалистам» (надеюсь, что слово *криптография* больше не оказывает на вас подобного воздействия).

Однако от важной роли прилагательного *квантовый* по отношению к криптографии прятаться не стоит. Оно возникает как минимум в трех разных контекстах, которые, несмотря на фундаментальные отличия между ними, часто путают. Первый из них касается существующих технологий разной степени практичности. Второй относится к важной технологии, которая еще не существует, но уже имеет большое значение. Третий контекст охватывает несуществующие технологии, которые вряд ли будут актуальными в ближайшем будущем.

Две потенциально полезные квантовые технологии, имеющие отношение к криптографии, уже существуют, и обе связаны с разными аспектами управления ключами. Первая – это *квантовая генерация случайных чисел*. Как мы уже видели, случайные числа чрезвычайно важны для криптографии, особенно для генерации ключей, и недетерминистические генераторы, основанные на естественных физических источниках, подходят лучше всего. Лучшие (или, по крайней мере, одни из лучших) инструменты этого рода основаны на квантовой механике[306]. Вторая технология направлена на решение проблемы с получением общего закрытого ключа в двух разных местах. *Квантовое распространение ключей* позволяет доставить ключ, сгенерированный случайным образом, из одного места в другое по специальному квантовому каналу.

В компьютерных технологиях назревает революция. *Квантовые компьютеры*, по всей видимости, будут способны выполнять некоторые задачи намного быстрее, чем нынешнее оборудование[307]. Это существенно повлияет на криптографию, так как криптографические операции, которые не по силам традиционным компьютерам, станут выполнимыми. На сегодня существует лишь несколько квантовых компьютеров с крайне ограниченными

возможностями, по сравнению с которыми карманный калькулятор может показаться суперкомпьютером. Но квантовые вычисления продолжат развиваться, поэтому мы должны относиться к ним серьезно и готовиться к тому моменту, когда они станут зрелыми.

Квантовые компьютеры будут способны взломать некоторые из криптографических алгоритмов, которые используются сегодня. Казалось бы, для решения этой проблемы было бы логично тоже обратиться к квантовым вычислениям. В конце концов, если квантовый компьютер способен взломать существующую криптографию, почему бы не разработать новые квантовые алгоритмы, которые будут выполняться на квантовых компьютерах? В этой идее нет ничего плохого, но в контексте защиты киберпространства она должна иметь довольно низкий приоритет.

У нас пока еще нет серьезных квантовых компьютеров, и появятся они, вероятно, нескоро. Но пройдет какое-то время, и квантовые компьютеры, может быть, будут применяться в нескольких технологически развитых организациях. Только у них будет возможность применять квантовые криптографические алгоритмы. Но намного важнее то, что всем остальным придется защищаться от этих нескольких квантовых устройств с помощью криптографии, которая работает на традиционных компьютерах. Пройдет еще какое-то время, и, возможно, квантовые вычисления станут чуть более распространенными. Только *тогда* в квантовых криптографических алгоритмах начнет появляться какой-то смысл. Со временем, вероятно, возможно, наверное… Я подозреваю, что эта проблема будет актуальна скорее для наших детей (или, может быть, даже их детей), чем для нас с вами.

Остерегайтесь разговоров более общего характера, касающихся *квантовой криптографии*. Этот абстрактный термин часто используется в отношении любого из контекстов, которые я описал в начале этого раздела, а то и всех трех сразу. Таким образом, квантовая криптография может уже существовать, а может и нет, может быть революционной или умозрительной, практичной или непрактичной. Вот почему я бы избегал этого термина. Однако мы не должны игнорировать квантовые компьютеры. Они все еще не умеют швырять злых птичек по свиньям[308], но у них есть потенциал стать настоящей катастрофой для современной криптографии.

Оружие массовой расшифровки

Кое-что о квантовых компьютерах *известно* уже сейчас. Они работают совершенно по-другому, чем традиционные вычислительные устройства. Данные, которые они обрабатывают, не нуждаются в переводе в двоичный код. Благодаря своей способности производить некоего рода операции параллельно они смогут выполнять задачи намного эффективней, чем их классические аналоги.

Однако многое о квантовых компьютерах все еще остается неизвестным. Мы не знаем, когда появятся квантовые компьютеры, пригодные для реального применения. Мы не знаем, смогут ли квантовые компьютеры достичь на практике всех тех целей, которые ставятся перед ними в теории. Мы не знаем, кто создаст первый практичный квантовый компьютер. Мы не знаем, как в итоге будет выглядеть внедрение квантовых компьютеров. Мы не знаем, станут ли они когда-либо обычной потребительской технологией. Но с точки зрения планирования будущего криптографии *все это неважно*. Главное, что квантовые компьютеры могут стать реальностью, и мы должны уже сегодня начинать разработку средств защиты от них[309].

Квантовые вычисления действительно будут иметь существенное влияние на современную криптографию, но они не отправят на свалку истории *все* криптографические технологии, которые мы используем сегодня. Некоторые алгоритмы, активно использующиеся сейчас, беззащитны перед квантовыми компьютерами, но другие по-прежнему остаются эффективными. Мы должны учитывать все эти прогнозы и понимать их возможные последствия.

Главная область риска – асимметричное шифрование и связанные с ним методы создания цифровых подписей. Почти все его разновидности, которые используются на сегодня, основаны на предполагаемой сложности двух математических задач: разложение на простые множители и поиск дискретных логарифмов. Достаточно мощный квантовый компьютер сможет эффективно справляться и с тем и с другим, что довольно прискорбно[310]. Иными словами, квантовые вычисления сделают все современные технологии асимметричного шифрования и создания цифровых подписей неэффективными.

Проблема с нынешними асимметричными алгоритмами шифрования в том, что их защищенность основана на конкретных вычислительных задачах, слишком сложных (по общему мнению) для традиционных компьютеров. Если появится настоящий квантовый компьютер, которому эти же задачи будут по зубам, у нас возникнут большие проблемы.

В связи с этим исследователи занимаются разработкой и анализом новых алгоритмов асимметричного шифрования, основанных на альтернативных вычислительных задачах, которые квантовые компьютеры не должны решать так же легко и эффективно. Эти *постквантовые* алгоритмы придут на смену технологиям, которые мы используем сегодня[311]. Аналогичные шаги предпринимаются для разработки новых постквантовых методов создания цифровых подписей. К этим технологиям предъявляется одно важное требование: они должны быть совместимы с традиционными компьютерами; квантовые методики как таковые в них не используются, однако они предназначены для того, чтобы защищать информацию от будущих злоумышленников с доступом к квантовым компьютерам.

С другими криптографическими инструментами ситуация получше. Защищенность алгоритмов симметричного шифрования обычно не зависит от какой-то одной вычислительной задачи. Они основаны, скорее, на разумном проектировании, чем на математике, и создают настолько сложную вычислительную преграду между исходными и зашифрованными данными, что вместо попыток взлома самого алгоритма лучше и логичнее сразу начинать поиски подходящего ключа.

Сегодня считается, что квантовый компьютер в лучшем случае сможет существенно ускорить простой перебор ключей, но не настолько, чтобы все современные алгоритмы симметричного шифрования разом стали неэффективными. В частности, высказываются предположения о том, что для защиты от злоумышленников с квантовыми компьютерами длину симметричных ключей придется удвоить[312].

Наиболее широко в современном киберпространстве используется алгоритм симметричного шифрования AES со стандартной длиной ключа 128 бит. Мы довольно много говорили о нем в этой книге. Однако AES поддерживает и 256-битные ключи, поэтому те, кто

опасается квантовых компьютеров, могут просто поменять этот параметр. Тем не менее часть широко распространенных систем не используют AES. В большинстве банковских и платежных сетей по-прежнему применяется алгоритм Triple DES, а у него ключи более короткие. Этим сетям, чтобы защититься от квантовых компьютеров, придется перейти на другие технологии симметричного шифрования.

Квантовые вычисления представляют реальную угрозу для криптографии, какой мы ее знаем и используем. Экстренные меры защиты от этой угрозы уже разрабатываются, и я убежден, что набор криптографических алгоритмов, способных противостоять квантовым компьютерам, будет разработан задолго до того, как эти компьютеры станут реальностью. Но до тех пор остается риск того, что данные, которые мы шифруем сегодня, могут быть завтра взломаны посредством квантовых вычислений.

Волшебные каналы

Технология, предоставляющая квантовое распространение ключей (англ. quantum key distribution – QKD), уже существует. Это не алгоритм шифрования, и в квантовом компьютере она тоже не нуждается. Суть технологии QKD в ее названии: это метод применения квантовой механики для распространения симметричного ключа.

Давайте еще раз пройдемся по основам проблемы распространения ключей. Два пользователя хотят обменяться зашифрованными сообщениями с помощью своего любимого алгоритма симметричного шифрования. Для этого каждому из них нужно каким-то образом получить копию одного и того же закрытого симметричного ключа. Один из вариантов состоит в том, что отправитель генерирует случайный ключ и передает его получателю. Но как это сделать?

В отсутствие телепатии это настоящая проблема. Отправитель не может просто передать ключ получателю по незащищенному каналу связи, так как злоумышленник может следить за этим каналом и перехватить ключ. Верно?

Не совсем. Этот аргумент применим к стандартным каналам связи, таким как сотовая сеть, Wi-Fi или Интернет. Но представьте, что речь

идет о «волшебном» канале, обладающем одним необычным свойством: если злоумышленник перехватит информацию, которая по нему проходит, получатель будет об этом оповещен (например, с помощью сигнала тревоги). Таким образом, отправитель может спокойно передать ключ получателю по волшебному каналу. Если сигнал тревоги не прозвучит, оба пользователя будут знать, что ключ не увидел никто лишний. В противном случае отправитель и получатель могут избавиться от ключа и повторить попытку.

Именно так устроен процесс QKD. «Волшебным» каналом в его случае выступает квантовое оптическое соединение, устанавливаемое с помощью лазеров прямой видимости или оптоволокна. Ключ кодируется в виде квантовых состояний, а благодаря свойствам квантовой механики любой, кто попытается прочитать данные в канале, непреднамеренно изменит эти состояния так, что позже получатель сможет это обнаружить[313]. QKD, вне всяких сомнений, одно из самых остроумных на сегодня применений квантовой механики. На основе этой технологии уже созданы разные экспериментальные сети, и с ее помощью происходит распространение ключей в космосе, через орбитальные спутники[314]. Коммерческие системы QKD уже доступны на рынке, хотя они далеко не дешевы.

Однако даже если технология захватывающая и новаторская, это еще не означает, что она нам действительно нужна. Суда на воздушной подушке, «Конкорд» и MiniDisc от Sony были блестящими изобретениями, которые решали реальные проблемы, но частью повседневной жизни они так и не стали. Средства QKD могут найти применение в нишевых сферах, но, увы, вполне вероятно, что они пополнят список технологий, которые больше обсуждают, чем применяют. И вот почему.

Во-первых, QKD – это дорогое решение проблемы, которую можно решить дешевле. QKD распространяет ключи для любых алгоритмов симметричного шифрования. Это замечательно, однако для этого существует множество других способов, включая предустановку долгосрочных ключей, из которых по мере необходимости генерируются ключи шифрования, как это происходит в мобильных телефонах, беспроводных сетях, банковских картах и других устройствах.

Есть мнение о том, что QKD может защитить нас от атак с использованием квантовых компьютеров, поскольку позволяет распространять ключи для специального алгоритма симметричного шифрования, известного как *шифр одноразовых блокнотов* или *шифр Вернама*. Теоретически этот алгоритм обладает максимальным уровнем защиты, возможным в симметричном шифровании, поскольку шифрует каждый бит исходных данных отдельно, используя случайный ключ[315]. К сожалению, использование шифра Вернама требует больших затрат, поскольку ему нужны случайные ключи, а они по длине равны исходным данным. Для большинства из нас нет никакого смысла заморачиваться распространением таких ключей, ведь, как уже отмечалось, алгоритм AES тоже устойчив к атакам квантового компьютера, и его ключи при этом относительно коротки.

Во-вторых, если говорить о будущем появлении квантовых компьютеров, QKD решает не ту проблему. Для использования QKD нужна статическая сеть с известным набором устройств, каждое из которых подключается с помощью специальной технологии. Именно в таком окружении для защиты сети будет достаточно симметричной криптографии. Но если квантовые компьютеры когда-либо станут реальностью, слабым местом будет вовсе не симметричное шифрование. Похоже, что квантовые вычисления создают необходимость в новых видах асимметричного шифрования. Нам нужны новые асимметричные алгоритмы для защиты соединений в открытых окружениях, таких как Всемирная паутина, где между сторонами взаимодействия не существует заранее определенных отношений. Соединения в открытых окружениях невозможно защитить с использованием QKD. Логично, что эта технология играет куда менее значительную роль в нашей будущей безопасности, чем разработка постквантовых алгоритмов асимметричного шифрования.

Криптография повсюду!

Надеюсь, теперь вы отдаете себе полный отчет о том, насколько важна криптография для защиты вашего пребывания в Интернете, ваших телефонных звонков, покупок с помощью банковских карт и т. д. Для большей части подобной деятельности необходима

криптография, так как все это происходит в разных областях того, что мы традиционно называем киберпространством.

Сейчас наблюдается тенденция к размытию границ между объектами, которые у нас прочно ассоциируются с киберпространством, включая компьютеры, планшеты, телефоны и другие повседневные вещи. Мы постепенно свыкаемся с мыслью о том, что телевидение, игровые консоли, часы и автомобили тоже становятся частью киберпространства. Мы уже (почти) готовы к тому, что к ним присоединятся термостаты, духовки, жалюзи и стиральные машины. Но действительно ли нам нужны солонки, зеркала, тостеры и мусорные ведра с подключением к Интернету, которые, между прочим, уже можно купить?[316]

Такую поддержку сетевого подключения у различных предметов иногда называют *Интернетом вещей* (англ. Internet of Things, или IoT). Это явление частично объясняется разработкой миниатюрных и доступных датчиков, которые можно встраивать в привычные для нас вещи. Поскольку к киберпространству можно подключить почти что угодно, и в большинстве случаев при этом требуется какой-то уровень безопасности, с популяризацией IoT криптография будет использоваться все более широко и во все более неожиданных местах[317].

Одна из сред, которые созрели для инноваций в сфере IoT – ваш дом. Уже доступны технологии, которые позволяют подключить к сети вашу бытовую технику, упрощая управление освещением, отоплением и другими электроприборами и делая их энергоэффективными. Вы, наверное, думаете, что вашим бытовым приборам не нужна особая безопасность, но подумайте еще раз. Информация в сети умного дома по большей части конфиденциальна. То, когда вы включаете и выключаете освещение и отопление, смотрите телевизор, готовите ужин и принимаете душ, позволяет получить представление о том, как проходит ваш типичный день. Немногие посчитают эти сведения интересными, но для тех, кто собирается вломиться к вам в дом, они бесценны.

Для получения корректного счета за электричество все эти данные должны быть правильными. Вам точно не захочется, чтобы к вашей сети имел доступ кто попало, иначе шутники превратят ваше жилище в дом с привидениями, где загадочным образом включается и

выключается свет, посреди ночи начинает греться духовка, а батареи, напротив, перестают греть в самую холодную пору. К счастью, кибердом можно защитить, надлежащим образом применяя криптографию. Будем надеяться, что те, кто разрабатывает все эти подключенные к сети технологии, обращают внимание на безопасность[318].

Одно из преимуществ умных духовок, выключателей с интернет-соединением и систем киберотопления в том, что все они имеют достаточно крупные габариты и могут поддерживать криптографию того же типа, которую мы используем в наших телефонах, банковских картах и автомобильных замках. О некоторых других устройствах, которые мы подключаем к Интернету, так не скажешь. Крошечные приспособления вроде RFID-меток (средств радиочастотной идентификации, которыми можно помечать товары) и миниатюрных беспроводных датчиков (у которых есть всевозможные способы применения, включая мониторинг сельскохозяйственных культур и отслеживание миграций диких животных) весьма ограничены в возможностях, если говорить о хранении и обработке данных. У них обычно мало памяти, и им нужно экономить электроэнергию, чтобы дольше проработать от аккумулятора.

Чтобы защитить такие устройства с помощью криптографии, исследователи работают над созданием специальных легковесных криптографических алгоритмов, тем более что в будущем может понадобиться что-то практически невесомое[319]. В таких алгоритмах обычно жертвуют какими-то аспектами безопасности в пользу повышения производительности по сравнению с традиционными аналогами. Это, пожалуй, допустимый компромисс, ведь вполне вероятно, что данные, собираемые такими устройствами, не нужно хранить в тайне долгое время. К тому же легковесная криптография лучше, чем вообще никакой.

Одно из последствий современного подхода к криптографии заключается в том, что для многих систем, с которыми вы взаимодействуете в киберпространстве, *роль криптографического ключа играете вы сами*. Банкомат выдаст деньги, только если система уверена в том, что чип на вставленной карте содержит ключ, который, как она считает, принадлежит вам. Кто бы ни сделал звонок с телефона, в который вставлена ваша SIM-карта, платить за него будете

вы. Ваш автомобиль откроет дверь любому, у кого есть криптографический ключ, привязанный к вашему брелоку.

Однако в будущем такая связь между человеком и его криптографическими ключами может стать еще теснее. Вы больше не будете представлены ключами – они будут содержаться в вашем теле, и, возможно, в больших количествах. Выиграют от применения технологий IoT, скорее всего, медицинские исследования и здравоохранение в первую очередь. В будущем к киберпространству среди прочих вещей будут подключены медицинские имплантаты, такие как электрокардиостимуляторы и другие средства мониторинга, как для наружного ношения, так и для внутреннего потребления. Эти технологии вполне могут передавать данные вашим мобильным медицинским приложениям, или непосредственно вашему врачу. *Internet of Me* (мой Интернет) – это уже не научная фантастика, а реальность. И эта область совершенно точно нуждается в защите, а значит, и в криптографии[320].

В 2012 году в одной из серий американского сериала *Родина* для покушения на вице-президента Уолдена злоумышленник подключается к его электрокардиостимулятору и ускоряет его сердцебиение. Эту серию, наверное, было не очень приятно смотреть тысячам зрителей с кардиостимуляторами по всему миру. Но, как и в случае с любыми другими будущими сферами использования IoT, при тщательном проектировании и внедрении криптографии их пульс, скорее всего, останется в норме. Мы можем защитить конфиденциальность медицинских баз данных и разработать кардиостимуляторы, которые будут взаимодействовать только с авторизованными медицинскими специалистами и допускать только безопасные параметры. Цель, стоящая перед обществом, состоит в том, чтобы вымышленные атаки оставались вымышленными.

Облачно, местами криптография

Когда-то мир был устроен так: вы генерировали данные (документы, фотографии, электронные письма – неважно) и хранили их на своем персональном компьютере, который находился под вашим контролем. Если вас беспокоила безопасность ваших данных, вы должны были

заниматься их защитой (используя криптографию, конечно). Это в равной степени относилось как к организациям, так и к частным лицам.

В наши дни все работает немного иначе: вы генерируете данные и сохраняете их где-то (неведомо где), позволяя контролировать их кому-то другому (неведомо кому). Вы можете обратиться к своим данным в любой момент и откуда угодно, их объем может многократно превышать емкость вашего локального хранилища на жестком диске. Именно так работают системы управления электронной почтой вроде Gmail, обмена файлами вроде Dropbox, музыкального вещания вроде Spotify и организации фотографий вроде Flickr. Необходимо отметить, что все больше организаций вверяют все свои данные заботе подобных сервисов, потому что это проще, дешевле и намного удобнее, чем поддерживать собственные системы. В целом эту концепцию принято называть *облаком*. Конечно, таких облаков много, но все они основаны на одних и тех же фундаментальных принципах.

Делегирование управления своими данными кому-то другому не обходится без очевидных рисков[321]. Тем не менее приличный провайдер облачных услуг должен серьезно относиться к кибербезопасности. На самом деле ваша информация может быть лучше защищена в облаке, чем на вашем собственном компьютере, так как вы можете попросту забыть об элементарных мерах предосторожности вроде резервного копирования. Однако в некоторых ситуациях (например, если дело касается базы данных с медицинскими записями) мы не хотим, чтобы провайдер облачных услуг мог просматривать данные, которые он для нас хранит. Очевидным решением будет шифрование данных перед их отправкой в облако.

К сожалению, хранение зашифрованной базы данных медицинских записей в облаке представляет собой серьезную проблему. Представьте, что нам нужно найти пациентов с определенной болезнью, отсортировать записи по дате рождения или вычислить средний возраст пациентов с определенными параметрами. Поскольку традиционные средства шифрования рассчитаны на генерацию непонятного шифротекста без видимой связи с оригиналом, эти операции нельзя проводить непосредственно с зашифрованной информацией. Таким образом мы должны загрузить зашифрованную

базу данных из облака, расшифровать ее и только затем выполнить наш анализ локально. Это неэффективный и неудобный процесс, так как облако нужно в первую очередь для того, чтобы избежать локального хранения всей этой информации.

Могло бы показаться, что потребность в криптографии подрывает некоторые преимущества облачных вычислений. Но на самом деле произошло кое-что поинтересней: необходимость в облачных вычислениях породила целую волну инноваций в области криптографии. Специально для ситуаций, подобных описанным выше, разрабатываются особые виды криптографических алгоритмов[322]. Например, *методы шифрования с возможностью поиска* позволяют владельцам данных искать нужную им информацию без предварительной расшифровки, а при использовании *гомоморфного шифрования* владельцы данных могут проводить с ними целый ряд вычислений (таких как сложение и умножение) и тоже без необходимости их расшифровывать. Шифрование данных с помощью этих методов делает возможной работу с ними прямо в облаке.

Методы шифрования с возможностью поиска позволяют проводить поиск по зашифрованной БД так, чтобы владельцу возвращались только найденные нужные элементы, которые затем расшифровываются локально. Гомоморфное шифрование позволяет владельцу данных вычислить среднее значение из каких-то числовых элементов внутри зашифрованной БД: для этого сначала вычисляется среднее зашифрованное значение (обычным образом), которое затем возвращается владельцу, а тот уже расшифровывает его локально, чтобы получить среднее значение для исходных данных. Эта возможность открывает путь для более сложных вычислений, таких как анализ зашифрованных данных.

Такого рода функционал по большому счету еще не готов к повсеместному применению, так как многие из этих новых криптографических методов пока недостаточно эффективны для широкого внедрения[323]. Тем не менее это показывает, насколько далеко ушла криптография с начала 1970-х годов, когда весь диапазон доступных средств состоял из симметричного шифрования. С возникновением в киберпространстве новых видов деятельности, имеющих определенные требования к безопасности, можно ожидать появления новых криптографических инструментов, предназначенных

для их защиты. Иными словами, в будущем криптография станет еще более распространенной, и будет предлагать еще больше возможностей.

Восстание машин

Мы часто слышим, что не за горами тот день, когда компьютеры могут стать умнее людей. Никто не знает, когда наступит *технологическая сингулярность* (кто-то говорит, что в 2030-х, а кто-то – в 2040-х)[324]. Никто не может предположить, будут эти суперумные компьютеры похожи на современные, или же мы придем к созданию цифровых киборгов, которые станут результатом слияния компьютерных сетей и человеческого мозга. Мы даже не можем точно сказать, что означает *умнее*, и заметим ли мы вообще технологическую сингулярность, если она когда-нибудь случится.

Но все это детали. Никто не станет спорить с тем, что компьютеры становятся способны решать все больше задач, которые раньше считались доступными только людям. В наше время компьютеры могут делать то, что было прерогативой человека всего пару десятилетий назад, включая интерпретацию человеческой речи или вождение автомобилей. Ожидается, что прогресс в области искусственного интеллекта только ускорит эту тенденцию. Уже можно себе представить роботов, способных ставить медицинские диагнозы, биноклей с возможностью идентифицировать все объекты в поле зрения, и полностью автоматизированных транспортных систем. Нравится нам это или нет, но искусственный интеллект неизбежно приведет к созданию многих вещей, которые мы пока даже не можем себе представить, и некоторые из них окажутся вне нашего контроля[325].

Мы сами ускоряем этот прогресс, генерируя все больше и больше данных. В 2018 году пользователи публиковали более 50 000 фотографий, писали более 500 000 твитов и отправляли 13 миллионов текстовых сообщений *каждую минуту*[326]. Такие огромные объемы информации и улучшения в алгоритмах, предназначенных для их

обработки и анализа, помогают компьютерам выполнять аналитические задачи, которые людям и не снились[327].

Что все это сулит будущему криптографии? Каким бы ни было внутреннее устройство и назначение компьютеров, для защиты данных им, вне всяких сомнений, и дальше будет нужна криптография. Может статься, они справятся лучше нас, и это позволит им гарантировать обеспечение надлежащей криптографической защиты.

Но есть еще один интересный вопрос: какое воздействие искусственный интеллект может оказать на саму криптографию[328]? Станут ли компьютеры в будущем настолько умными, что им будет под силу взломать любые известные криптографические алгоритмы подобно суперкомпьютеру из романа Дэна Брауна *Цифровая крепость*?

Сомневаюсь. Угроза криптографии возникает в результате несоответствия возможностей тех, кто ею пользуется, и тех, кто пытается ее взломать. Чтобы это проиллюстрировать, стоит вспомнить такие несоответствия, которыми пользовались правительства для контроля за использованием шифрования. В 1950-х и 1960-х годах государство имело намного больше опыта разработки криптографических средств. В 1970-х и 1980-х государство имело возможность ограничить устойчивость и распространение криптографических технологий на уровне законодательства. В наше время информация, раскрытая Сноуденом, показывает, что преимущество правительственных служб заключается в наличии общей картины того, как используется криптография, и возможности политического давления на основных поставщиков технологий. Если нам не удастся создать алгоритмы асимметричного шифрования, устойчивые к квантовым вычислениям, в будущем аналогичное несоответствие может быть выражено в доступе к квантовым компьютерам.

Я легко могу себе представить, что развитие искусственного интеллекта и автоматизации формулирования логических выводов станет угрозой для современной криптографии. Чрезвычайно сложные компьютерные программы вполне могут научиться проводить более тщательный анализ безопасности криптосистем, чем мы способны даже представить сегодня. Это может сделать доступным поиск тонких уязвимостей, для выявления которых приходится проводить глубокое

исследование. Такие программы могут находить в зашифрованных данных неочевидные закономерности. Но чтобы прогресс в области искусственного интеллекта привел к несоответствию возможностей, должна появиться машина, способная выполнять атаки, о которых мы даже не догадываемся. Я не могу сказать, что этого никогда не произойдет, но мне кажется, что современный научный прогресс происходит в достаточно открытой среде и в тесном сотрудничестве, поэтому вряд ли кому-то удастся сохранять подобные возможности в тайне действительно долго.

Зная, что нам угрожает, мы можем что-то предпринять. Если умные компьютеры сделают скачок вперед с точки зрения *взлома* криптографии, мне кажется, что этот ум почти наверняка позволит нам усовершенствовать процесс ее *разработки*. Современная криптография разрабатывается людьми, а компьютеры используются для моделирования и тестирования ее защищенности. В будущем компьютеры вполне могут превзойти нас в этом созидательном процессе и создать более устойчивые криптографические средства, которые будут проходить более тщательную проверку. Скорее всего, они смогут лучше анализировать целые компьютерные системы, определяя, какие криптографические технологии следует применять и как их реализовывать.

Прогресс в области криптографии иногда называют «гонкой» между созидателями и разрушителями. Криптографические технологии должны совершенствоваться, чтобы противостоять методам взлома, которые тоже не стоят на месте. По моему мнению, чтобы удерживать лидерство, созидателям нужно следить за тем, как развиваются приемы разрушения. Если разработчики криптосистем не будут игнорировать прогресс в сфере искусственного интеллекта, то криптографии, которая будет лежать в основе будущих вычислительных потребностей, окажется достаточно. Однако ни у кого из живущих сегодня нет ни малейшего представления о том, как сложится будущее искусственного интеллекта.

Доверие к криптографии

Если в нашем криптографическом будущем и должно что-то измениться действительно серьезно, так это понятие *доверия*[329]. Криптография тесно связана с доверием, и наша будущая безопасность в конечном счете зависит от того, станет ли эта связь еще теснее. Важно понимать, чем это обусловлено.

Доверие – это «твердая убежденность в надежности, достоверности или способности чего-то или кого-то»[330]. Именно это обеспечивает криптография в киберпространстве. Нам нужно понимать, кто и что знает, какая информация корректна и кто с кем взаимодействует. Учитывая природу киберпространства, доверие невозможно выстроить *без* криптографии.

Криптография тоже *опирается* на доверие. Чтобы она работала, мы должны доверять утверждению о том, что определенные математические вычисления сложно выполнять на компьютере. Мы должны верить в то, что вычислительные ресурсы злоумышленника не превышают ожидаемого уровня. Мы должны довериться тому, что пользователи криптографии будут вести себя предсказуемо и не станут, к примеру, публиковать свои криптографические ключи в социальных сетях.

В целом же криптография сама по себе нуждается в доверии. Информация, которую раскрыл Сноуден в 2013 году, существенно подорвала доверие общества к криптографии[331]. Как уже отмечалось, процессу разработки криптографических алгоритмов действительно не всегда можно доверять. То же самое относится к их реализации в современных технологиях или процедурам управления ключами. Если мы не верим в надежность криптографии, можно ли надеяться на установление реального доверия в киберпространстве?

Установление доверия в криптографии – задача не самая простая. Существенным препятствием служит очень высокая сложность того, чему мы должны довериться. И речь идет не только об алгоритмах; мы должны доверять всей системе, в которой применяется криптография, включая производителей технологий и операторов сетей, в которых эти технологии развертываются. Все это усугубляется тем, что разные люди доверяют или не доверяют очень разным вещам[332].

Тем не менее некоторые положительные тенденции свидетельствуют о том, что мы двигаемся в правильном направлении.

Одна из этих тенденций связана с выбором. Парламентская демократия – это система государственного управления, популярность которой помимо прочего объясняется возможностью граждан выбирать своих представителей. Мы не всегда доверяем нашим политикам, но они, наверное, заслуживают больше доверия, чем правители, которые удерживают власть силой. В середине 1970-х в криптографии почти не из чего было выбирать. Если вам нужно было симметричное шифрование, едва ли не единственным вариантом был алгоритм DES. Сегодня же мы можем выбирать любой из десятков доступных алгоритмов симметричного шифрования. Выбор не означает гарантий безопасности, но он укрепляет доверие.

Технологии, которые используются для защиты телекоммуникационных сетей 4G и 5G, позволяют выбирать криптографические алгоритмы; в частности, в Китае был разработан специальный алгоритм для внутреннего использования. По всей видимости, китайцы не доверяют криптографическим алгоритмам, созданным за рубежом (а кто-то другой, несомненно, не доверяет китайским алгоритмам), однако наличие их собственного алгоритма в спецификации способствует укреплению доверия к безопасности телекоммуникаций внутри Китая. Точно так же вы можете сконфигурировать параметры безопасности TLS в своем браузере, чтобы для установления безопасных соединений с сервером использовались только те алгоритмы, которым вы доверяете.

Второй тенденцией стал повышенный интерес (как в научных кругах, так и среди практикующих специалистов) к безопасному применению криптографии в реальных технологиях. В прошлом безопасность криптографии оценивалась в отрыве от окружения, в котором она использовалась. Сейчас при анализе алгоритмов учитывается общая криптосистема, в рамках которой они работают. Например, давая оценку криптографическому протоколу вроде TLS, мы не просто проверяем его корректность и способность достичь заявленного уровня безопасности, но и следим за тем, чтобы эти свойства сохранялись после его реализации в реальной среде, где находчивый злоумышленник может пользоваться вспомогательной информацией, например сообщениями об ошибках. Существует несколько ежегодных мероприятий, которые собирают специалистов для обсуждения теории криптографии, однако крупнейшей в этой

сфере считается конференция *Real World Crypto Symposium*, где сотни исследователей и разработчиков совместно расширяют свое коллективное понимание того, как укрепить доверие к криптографии, применяемой для защиты широко распространенных технологий[333].

После поступка Сноудена пользователи стали менее беспечными, и это, как мне кажется, самое главное. Этот сдвиг включает в себя более глубокое осознание того, что нам нужна криптография, которой мы можем доверять. Споры о сквозном шифровании, продолжающиеся между правительствами и поставщиками технологий – только один из примеров. Еще один пример, наверное, состоит в том, что вы читаете эту книгу.

Верите ли вы в то, что безопасность, которую обеспечивает криптография, соответствует вашим потребностям? Я показал вам довольно много признаков и причин того, что в это стоит верить, пусть и с некоторыми оговорками. Если мы стремимся создать не просто безопасный криптографический алгоритм, но защищенную криптосистему, в которой работает его безопасная реализация, то в будущем доверие к криптографии может только укрепиться. По крайней мере я на это надеюсь.

Криптография и вы

А что насчет вашего личного криптографического будущего? Всегда полезно знать, какую роль криптография играет в кибербезопасности. Но следует ли вам просто продолжать свою деятельность в киберпространстве, будучи уверенным в том, что криптография «делает свое дело» для вашей защиты?

Прежде всего, я надеюсь, что, сняв завесу тайны с криптографии, я избавил вас от страха перед неизвестным. Тема кибербезопасности доступна для понимания не только компьютерным гениям. Криптография предоставляет фундамент, на котором основаны технологии безопасности. Имея представление о том, как она работает, вы уже обладаете некоторыми основополагающими знаниями об организации безопасности в киберпространстве.

Я надеюсь и на то, что знания о криптографии изменят ваши взгляды на кибербезопасность. Ее анализ через криптографическую

призму может быть очень полезным. Вы теперь знаете, что, когда ваш банк выдает вам устройство для онлайн-доступа к вашему счету, вы на самом деле получаете алгоритм и уникальный ключ. Контролируя это устройство, вы можете входить в систему намного более безопасным путем, чем, скажем, при вводе PIN-кода и девичьей фамилии матери.

Криптографическое мышление может помочь вам разобраться в текущих событиях. Если в новостях о технологии, которую вы используете, звучит слово «взлом», не всегда ясно, в чем именно заключается проблема. Возможно, использовался плохой криптографический алгоритм, может, ключи генерировались неправильно, а может, эти ключи были попросту украдены с сервера? Стоит ли вам лично предпринимать какие-то меры, или лучше подождать, пока поставщик технологии не решит проблему? Достаточно ли поменять пароль, или стоит перейти на другую технологию?

Знание основ криптографии также должно придать вам уверенность, необходимую для оценки вашего текущего подхода к кибербезопасности. Как защищены данные на ваших устройствах? Обеспечены ли сетевые соединения, направленные к вашему сайту, криптографической защитой? Насколько легко кому бы то ни было представиться «вами» в киберпространстве? Вы можете даже пойти на упреждающие меры. Если на вашем ноутбуке есть по-настоящему конфиденциальные данные, их, пожалуй, лучше зашифровать. Если вы регулярно записываете конфиденциальную информацию на флешки, вам, возможно, стоит приобрести носители с криптографической защитой.

Что не менее важно, вы можете применять свои знания криптографии при выборе технологий или услуг, которыми вы хотите пользоваться в будущем. Задайте себе неловкие вопросы. Какой уровень безопасности они предоставляют? Какие они используют алгоритмы? Кто генерирует ключи, и где эти ключи хранятся? Ответы на эти вопросы найти не всегда легко, но поставщики все чаще публикуют подробности о предоставляемых ими продуктах, так как становится очевидным тот факт, что безопасность, помимо своей основной функции, еще и делает продукт привлекательней. Учитывайте криптографию при выборе того, что использовать и чем заниматься в киберпространстве.

Понимание того, какую роль криптография играет в кибербезопасности, тоже должно помочь вам сделать свой вклад в общественную дискуссию о ее использовании. Я призываю вас сформировать свое собственное мнение о том, как общество должно совмещать стремление к безопасности и конфиденциальности в киберпространстве. Это не означает, что вы должны стать политиком. Важные проблемы лучше всего решать одновременно на высоком уровне и на местах. Например, для борьбы с глобальным потеплением необходимо сочетание глобального политического руководства и ежедневных изменений, которых добивается каждый отдельный человек. Эти вещи взаимосвязаны, так как индивидуальные действия могут влиять на политику, а политика может изменять поведение людей. Следовательно, вы тоже можете поучаствовать в дискуссии о безопасности и конфиденциальности, включая контроль за использованием криптографии. Вы это делаете, когда решаете, какую информацию публиковать в Интернете, с какими технологиями иметь дело и как реагировать на новости и события из сферы безопасности. Высказывайте свое мнение и не позволяйте другим определять ваше будущее за вас.

Помните о криптографии и о том, как она вам может послужить. Сегодня на нее опирается наша безопасность, и в будущем эта зависимость только усилится.

Благодарности

У этой книги было три невольных вдохновителя.

Первым был мой отец. Будучи оптимистом, я надеялся, что моя первая (более академичная) книга о криптографии будет доступна широкому кругу эрудированных читателей. Вежливое замечание отца о том, что ему удалось лишь выборочно пройтись по тексту, было явным признаком того, что для более широкой аудитории потребуется совершенно другой подход. Я считаю, что данная книга прошла «проверку папой».

Вторым вдохновителем стал Эдвард Сноуден. Поступок, который он совершил в 2013 году, вызвал дискуссию мирового масштаба об использовании криптографии, и в ходе последующего анализа я был поражен тем, какой дискомфорт вызывала эта тема у многих журналистов и политиков.

Третий вдохновитель – анонимный литературный агент, который, прочитав мои статьи на сайте *The Conversation*, предложил мне написать научно-популярную книгу о кибербезопасности. Будьте осторожны в своих желаниях!

Мне повезло поработать с Питером Таллаком из The Science Factory, который с самого начала верил в этот проект и познакомил меня с издательским миром вне академических кругов. Томас Рид сказал, что издательство Norton будет отличным выбором, и оказался прав. Огромное спасибо моему редактору, Куин До, за ее неиссякаемый энтузиазм и поддержку, а также Дрю Вайтман за эффективную организацию всего процесса. Еще я в большом долгу перед Стефани Гиберт, которая внимательнейшим образом вычитала черновик.

Любая книга нуждается в читателях. Я чрезвычайно признателен за отзывы, которые мне прислали Сью Барвик, Никола Бейт, Ликуин Чен, Джейсон Крэмптон, Анни Кроу, Бен Кертис, Марис Элфик, Стивен Гэлбрейт, Вен-Ай Джексон, Энгус Хендерсон, Талия Лэйн, Генри Мартин, Иэн Маккиннон, Кенни Патерсон, Маура Патерсон и Ник Робинсон. Хотелось бы отдельно поблагодарить Коллин Маккена за ее тщательный анализ моих навыков словесности и Фреда Пайпера за то, что проверил своим зорким глазом мою криптографию. Ваше

совместное одобрение придало мне уверенности в том, что мне все-таки удалось сбалансировать эти два аспекта.

Напоследок выражаю особую признательность Рамону, моей таксе, за то, что он преданно сидел рядом со мной, пока эти слова медленно и с трудом появлялись на экране моего ноутбука, Кайле и Финлэй за то, что позволяли мне отвлечься в ходе этого процесса, и Аните за ее неизменные любовь и веру, несмотря ни на что.

* * *

КИТ МАРТИН

КРИПТОГРАФИЯ

КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ

АЛГОРИТМЫ ШИФРОВАНИЯ | МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ | ПРОТОКОЛЫ БЕЗОПАСНОСТИ

БОМБОРА
издательство

Примечания

1

Дэми Ли, «Apple Says There Are 1.4 Billion Active Apple Devices», *Verge*, 29 января 2019 года, **https://www.theverge.com/2019/1/29/18202736/apple-devices-ios-earnings-q1–2019**.

Вернуться

2

По состоянию на апрель 2018 года в мире существовало 7,1 миллиарда глобальных банковских карт EMV (Europay, Mastercard и Visa) с чипом и PIN-кодом: «EMVCo Reports over Half of Cards Issued Globally Are EMV® Enabled», EMVCo, 19 апреля 2018 года, **https://www.emvco.com/wp-content/uploads/2018/04/Global-Circulation-Figures_FINAL.pdf**.

Вернуться

3

Это цифры, которые компания WhatsApp опубликовала в середине 2017 года, но даже если они немного преувеличены, они, скорее всего, правильно отражают масштаб: WhatsApp, «Connecting One Billion Users Every Day», *Блог WhatsApp*, 26 июля 2017 года, **https://blog.whatsapp.com/connecting-one-billion-users-every-day**.

Вернуться

4

По сообщениям компании Mozilla, в 2018 году доля веб-страниц, загруженных браузерами Firefox по https (с шифрованием), достигла

отметки в 75 процентов: Let’s Encrypt Stats, Let’s Encrypt, по состоянию на 10 июня 2019 года, **https://letsencrypt.org/stats**.

Вернуться

5

Энигма (режиссер Майкл Эптед, Jagged Films, 2001) – художественный фильм о криптографах, работавших в Блетчли-парке, Англия, во время Второй мировой войны, и их попытках расшифровать переговоры, закодированные нацистскими машинами Энигма. В фильме *007: Координаты «Скайфолл»* (режиссер Сэм Мендес, Columbia Pictures, 2012) Джеймс Бонд и его квартирмейстер, Q, занимаются впечатляющим (и несколько неправдоподобным) анализом зашифрованных данных. Фильм *Тихушники* (режиссер Фил Алден Робинсон, Universal Studios, 1992), пожалуй, опередил свое время; в нем два студента занимаются взломом компьютерных сетей и оказываются вовлечены в сбор разведданных с использованием устройств, способных взламывать криптографию.

Вернуться

6

C.S.I.: Киберпространство (Jerry Bruckheimer Television, 2015–16) – американский драматический сериал об агентах ФБР, расследующих киберпреступления. В нем изображены довольно необычные криптографические методики, включая хранение ключей шифрования в виде татуировок. *Призраки* (Kudos, 2002–11) или *MI-5* – британский телесериал о вымышленных сотрудниках спецслужб. В нескольких сериях агенты имеют дело с зашифрованными данными, демонстрируя необычайный талант к преодолению шифрования прямо на лету!

Вернуться

7

Дэн Браун использовал криптографию в нескольких своих книгах, особенно в романе *Цифровая крепость* (St. Martin's Press, 1998), посвященном компьютеру, способному взломать любой известный метод шифрования. Интересно, что в самом известном романе Брауна, *Код да Винчи* (Doubleday, 2003), одним из персонажей выступает криптограф, хотя криптографии как таковой там нет.

Вернуться

8

Мой коллега Роберт Каролайна считает, что киберпространство – это не место, а средство взаимодействия. Он приводит сравнение между *киберпространством* и термином *televisionland*, с помощью которого на заре телевидения описывали абстрактную связь между людьми и новой технологией. В наши дни приветствие «Доброе утро всем в телевиделяндии!» (фраза, с которой экипаж *Аполлон-7* начал свое первое радиообращение из космоса в 1968 году); Каролайна ожидает, что идея нахождения «в киберпространстве» точно так же в конечном счете выйдет из употребления. Я склонен с ним согласиться.

Вернуться

9

Киберпространство – это концепция, которой чрезвычайно сложно дать четкое определение. Принято считать, что впервые этот термин использовал писатель Уильям Гибсон, однако современные определения обычно основаны на абстрактном описании компьютерных сетей и данных, которые в них находятся. В своем выступлении на *Crypto Wars 2.0* (третий межуниверситетский семинар по кибербезопасности, Оксфордский университет, май 2017 года) доктор Киан Мерфи (Бристольский университет) предложила более краткое определение: «Мне не нравится слово *киберпространство*, я предпочитаю называть это *электронными вещами*».

Вернуться

10

Согласно Internet World Stats (Miniwatts Marketing Group), по состоянию на 14 июля 2019 года, **https://www.internetworldstats.com/stats.htm**, чуть более половины населения мира уже в Интернете.

Вернуться

11

«2017 Norton Cyber Security Insights Report Global Results», Norton by Symantec, 2018, **https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf**.

Вернуться

12

Почти каждая вторая организация утверждает, что она была жертвой мошенничества и экономических преступлений, 31 % из этих случаев относится к киберпреступности: «Pulling Fraud Out of the Shadows: Global Economic Crime and Fraud Survey 2018», PwC, 2018, **https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html**.

Вернуться

13

Это внушительная оценка того, что нельзя измерить. Но она отражает идею о том, что в связи с нашей повышенной активностью в киберпространстве возрастает вероятность того, нас там кто-то обманет. Эти конкретные цифры взяты из отчета по киберпреступности за 2017 год, Cybersecurity Ventures,

https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

Вернуться

14

Компьютерное вредоносное ПО Stuxnet использовалось для атаки на завод по обогащению урана в Нетензе, Иран, в котором в начале 2010 года начали замечать неполадки. Это, пожалуй, первый общеизвестный пример того, как важный индустриальный объект стал жертвой атаки из киберпространства. Это не только усилило напряжение вокруг данного инцидента в сфере международной политики и ядерной безопасности, но и послужило напоминанием всему миру о том, что критически важная национальная инфраструктура все чаще подключена к киберпространству. Атака на Нетенз проводилась не напрямую через Интернет, а, как считается, была инициирована с помощью зараженных USB-накопителей. О Stuxnet и Нетензе много всего написано – например, см. *Countdown to Zero Day: Stuxnet, and the Launch of the World's First Digital Weapon*, Ким Зиттер (Broadway, 2015).

Вернуться

15

В ноябре 2014 года компания Sony Pictures Studios подверглась целому ряду кибератак, которые привели к раскрытию конфиденциальных сведений о ее сотрудниках и удалению данных. Злоумышленники требовали от Sony остановить выход нового комедийного фильма о Северной Корее. Например, см. статью Андреа Питерсон «The Sony Pictures Hack, Explained» в *Washington Post* от 18 декабря 2014 года, **https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b25b19d65b8d**.

Вернуться

16

Широко освещавшиеся атаки с *переустановкой ключей* были направлены на протокол безопасности WPA2, который использовался для криптографической защиты сетей Wi-Fi: Мэти Ванхоф, «Key Reinstallation AttacksWPA2 by Forcing Nonce Reuse», последнее обновление в октябре 2018 года, **https://www.krackattacks.com**.

Вернуться

17

Атака *ROCA* использует уязвимость в криптографической программной библиотеке для генерации ключей RSA, которые использовались в смарт-картах, токенах безопасности и других защищенных чипах производства Infineon Technologies. В результате появлялась возможность восстановить закрытые ключи для расшифровки: см. отчет Петра Свенды, «ROCA: Vulnerable RSA Generation (CVE15361)», опубликованный 16 октября 2017 года, **https://crocs.fi.muni.cz/public/papers/rsa_ccs17**.

Вернуться

18

Эксплойты *Meltdown* и *Spectre* использовали слабые места в широко распространенных компьютерных чипах. В январе 2018 года стало известно, что они затрагивают миллиарды устройств по всему миру, включая модели iPad, iPhone и Mac: «Meltdown and Spectre: All Macs, iPhones and iPads affected», BBC, 5 января 2018 года, **http://www.bbc.co.uk/news/technology-42575033**.

Вернуться

19

Кибератака *WannaCry* навредила многим старым компьютерам в Национальной службе здравоохранения Великобритании (и не только). В ходе нее устанавливался вирус-вымогатель, который шифровал диски зараженных устройств и затем вымогал выкуп взамен на расшифровку данных, которые стали недоступными. Позже Национальное аудиторское управление опубликовало детали расследования этого происшествия и предложило несколько способов, как его можно было бы избежать: Амьяс Морс, «Investigation: WannaCry Cyber Attack and the NHS», Национальное аудиторское управление, 25 апреля 2018 года, **https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs**.

Вернуться

20

Коми стал своего рода легендой в кругах специалистов по кибербезопасности за высказывания относительно его обеспокоенности о том, что использование криптографии мешает органам правопорядка. Например, в сентябре 2014 года он, как сообщается, выразил озабоченность усилением средств шифрования на различных мобильных устройствах: Райан Рейли, «FBI Director James Comey 'Very Concerned' about New Apple, Google Privacy Features», *Huffington Post*, 26 сентября 2014 года, **http://www.huffingtonpost.co.uk/entry/james-comey-apple-encryption_n_5882874**. В своем заявлении в мае 2015 года Коми по сообщениям журналистов был огорчен еще сильнее: Лорензо Франчески-Биккераи, «Encryption Is 'Depressing,' the FBI Says», *Vice Motherboard*, 25 мая 2015 года, **https://motherboard.vice.com/en_us/article/qkv577/encryption-is-depressing-the-fbi-says**.

Вернуться

21

Нравится вам Сноуден или нет, опубликованная им информация имела далеко идущие последствия, и я подробно поговорю о ней позже, когда речь пойдет о дилемме, возникшей из-за применения криптографии.

Вернуться

22

Вот что ответил Кэмерон на свой собственный вопрос: «Нет, мы не должны». Это замечание было воспринято многими как предложение запретить технологии шифрования: Джеймс Болл, «Cameron Wants to Ban Encryption – He Can Say Goodbye to Digital Britain», *Guardian*, 13 января 2015 года, **https://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror**.

Вернуться

23

Брэндис сделал это заявление перед совещанием разведывательного альянса *Пять глаз*: Крис Дакетт, «Australia Will Lead Five Eyes Discussions to ‘Thwart’ Terrorist Encryption: Brandis», ZDNet, 26 июня 2017 года, **https://www.zdnet.com/article/australia-will-lead-five-eyes-discussions-to-thwart-terrorist-encryption-brandis**.

Вернуться

24

Кирен Маккарти, «Look Who’s Joined the Anti-encryption Posse: Germany, Come On Down», *Register*, 15 июня 2017 года, **https://www.theregister.co.uk/2017/06/15/germany_joins_antiencryption_posse**.

Вернуться

25

«Attorney General Sessions Delivers Remarks to the Association of State Criminal Investigative Agencies 2018 Spring Conference», Министерство юстиции США, 7 мая 2018 года, **https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-association-state-criminal-investigative**.

Вернуться

26

Зейд заявил: «Средства шифрования широко используются по всему миру, в том числе защитниками прав человека, гражданским обществом, журналистами, осведомителями и политическими диссидентами, которым грозят преследования и притеснения. Шифрование и анонимность необходимы как для свободы выражения мнений, так и для права на частную жизнь. Утверждение о том, что без средств шифрования под угрозой могут оказаться человеческие жизни, не является ни надуманным, ни преувеличенным. В самом худшем случае способность правительственных органов взламывать телефоны своих граждан может привести к преследованиям тех, кто всего лишь пользуется своими неотъемлемыми правами». «Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid», канцелярия верховного комиссара ООН по правам человека, 4 марта 2016 года, **http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138**.

Вернуться

27

«The Historical Background to Media Regulation», открытый архив Лестерского университета, данные по состоянию на 10 июня 2019 года, **https://www.le.ac.uk/oerresources/media/ms7501/mod2unit11/page_02.htm**.

Вернуться

28

Бывший Министр внутренних дел Великобритании Эмбер Радд сделала об этой проблеме довольно откровенное заявление: «Мне не нужно знать, как работает шифрование, чтобы понимать, как оно помогает (сквозное шифрование) преступникам». Брайан Уиллер, «Amber Rudd Accuses Tech Giants of 'Sneering' at Politicians», BBC, 2 октября 2017 года, **http://www.bbc.co.uk/news/uk-politics-41463401**.

Вернуться

29

О богатой и увлекательной истории криптографии написано множество книг. Одна из самых доступных – *The Code Book* (Fourth Estate, 1999) авторства Саймона Сингха. Эталоном по-прежнему остается книга Дэвида Кана *The Codebreakers* (Scribner, 1997), но можно выделить и *World War II Cryptography* (CreateSpace, 2016) от Charles River Editors, *Unsolved!* (Princeton University Press, 2017) Крейга Бауэра, *Codes and Ciphers – A History of Cryptography* (Hesperides, 2015) Александра Д'Агапейеффа и *Codebreaker: The History of Codes and Ciphers* (Walker, 2006) Стивена Пинкока. В своей книге *Decipher: The Greatest Codes Ever Invented and How to Break Them* (Modern Books, 2017) Марк Фрари проводит хронологическое исследование ряда исторических кодов и шифров. В превосходной книге Стивена Леви *Crypto: Secrecy and Privacy in the New Cold War* (Penguin, 2000) задокументированы американские политические события второй половины двадцатого века, связанные с криптографией.

Вернуться

30

Существуют разные книги, посвященные криптографическим головоломкам. Например, *The GCHQ Puzzle Book* (GCHQ, 2016), *Break the Code* (Dover, 2013) Бада Джонсона и *Cryptography: The Science of Secret Writing* (Dover, 1998) Лоуренса Д. Смита.

Вернуться

31

Если этот шифр вам не поддался, попробуйте сдвинуть буквы вперед на одну позицию в алфавите! – *Здесь и далее прим. ред.*

Вернуться

32

Многие национальные монетные дворы предоставляют подробности о мерах защиты валюты, чтобы помочь с обнаружением подделок. Это относится как к тактильным ощущениям, так и к внешнему виду купюр. Больше о мерах защиты монет Британского фунта можно узнать в статье «The New 12-Sided £1 Coin» от Королевского монетного двора, **https://www.royalmint.com/new-pound-coin** (по состоянию на 10 июня 2019 года); в статье «Take a Closer Look – Your Easy to Follow Guide to Checking Banknotes» от Банка Англии, **https://www.bankofengland.co.uk/-/media/boe/files/banknotes/take-a-closer-look.pdf** (по состоянию на 10 июня 2019 года) речь идет о британских купюрах; а о долларе США можно почитать в документе «Dollars in Detail – Your Guide to U.S. Currency», опубликованном в рамках Образовательной программы о национальной валюте США, **https://www.uscurrency.gov/sites/default/files/downloadable-materials/files/CEP_Dollars_In_Detail_Brochure_0.pdf** (по состоянию на 10 июня 2019 года).

Вернуться

33

Генеральный фармацевтический совет Великобритании устанавливает стандарты для фармацевтов. Стандарт под номером 6 гласит: «фармацевты должны вести себя профессионально»; это означает вежливость, тактичность, проявление сочувствия и сострадания, уважительное отношение к людям и защита их достоинства. См. «Standards for Pharmacy Professionals», Генеральный фармацевтический совет, май 2017 года, **https://www.pharmacyregulation.org/sites/default/files/standards_for_pharmacy_professionals_may_2017_0.pdf**.

Вернуться

34

Это не совсем точно, поскольку людям свойственно переоценивать одни угрозы, такие как авиакатастрофы, и существенно недооценивать другие, например, загрязнение воздуха.

Вернуться

35

В 2016 году объем финансового мошенничества с платежными картами, удаленным банкингом и чеками в Великобритании оценивался в размере 768,8 миллиона фунтов: «Fraud: The Facts, 2017», Financial Fraud Action UK, 2017, **https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf**.

Вернуться

36

Для нашего читателя этот раздел может быть довольно забавен, поскольку именно такие аферы с платежками в последние несколько лет происходят постоянно и массово.

Вернуться

37

Стефани Хоэл и др., «Itsy Bitsy Spider. .: Infants React with Increased Arousal to Spiders and Snakes», *Frontiers in Psychology* 8 (2017): 1710.

Вернуться

38

«9/11 Commission Staff Statement No. 16», Комиссия по событиям 11 сентября, 16 июня 2004 года, **https://www.9–11commission.gov/staff_statements/staff_statement_16.pdf**.

Вернуться

39

Королевство Руритания – вымышленная страна центральной Европы, в которой происходит действие романа *The Prisoner of Zenda* Энтони Хоупа, 1894 год. Я взял на себя смелость использовать Руританию в качестве типичного государства, чтобы не обидеть ничьи национальные чувства. Я (бесстыдно) скопировал этот прием у моего коллеги Роберта Каролайна, который использовал Руританию в своих курсах по киберзаконодательству.

Вернуться

40

Появляется все больше и больше рекомендаций о том, как распознавать поддельные электронные сообщения. Например, см. «Protecting Yourself», Get Safe Online, **https://www.getsafeonline.org/protecting-yourself** (по состоянию на 10 июня 2019 года).

Вернуться

41

Программное обеспечение, написанное для сбора и использования информации о ничего не подозревающем пользователе часто называют *шпионским ПО*. Это могут быть как относительно невинные программы слежения, предназначенные для подбора адресной рекламы, так и системы мониторинга, сообщающие сторонним лицам о любой активности, включая случайные нажатия клавиш.

Вернуться

42

Общий недостаток понимания того, как устроено киберпространство, вредит отдельным людям, но это, наверное, создает еще более хронические проблемы для общества в целом. В отчете правительства Великобритании освещаются экономические потери, вызванные общей нехваткой цифровых навыков, и выявляется необходимость существенно улучшить обучение в этой сфере в школах, вузах и на производстве: «Digital Skills Crisis», комитет по науке и технике палаты общин Великобритании, 7 июня 2016 года, **https://publications.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf**.

Вернуться

43

В 2010 году датский веб-сайт под названием Please Rob Me (дословно, «пожалуйста, ограбь меня») вызвал много споров, объединив ленты из социальных сетей и мобильного геолокационного приложения, в результате чего получился список адресов потенциально пустых домов. Создатели утверждали, что это делалось для повышения уровня осведомленности пользователей, но многие осудили эту инициативу, назвав ее безответственной. И хотя инструмент *PleaseRobMe* давно не существует, количество геолокационных приложений только увеличилось, а возможности по объединению источников данных для получения такого рода информации стали намного эффективней. См. Дженнифер Ван Гроув,

«Are We All Asking to Be Robbed?», Mashable, 17 февраля 2010 года, **https://mashable.com/2010/02/17/pleaserobme**.

Вернуться

44

В качестве одного из многочисленных примеров можно привести следующую ситуацию: в 2016 году платформа под названием *Avalanche* была закрыта международным объединением правоохранительных органов. Она размещалась в восточной Европе и управляла сетью взломанных компьютерных систем, из которых можно было осуществлять различные киберпреступления, включая такие атаки как фишинг, спам, вымогательство и DoS. По оценкам, максимальное количество компьютеров, контролируемых платформой Avalanche, достигало полумиллиона: Уорик Эшфорд, «UK Helps Dismantle Avalanche Global Cyber Network», *Computer Weekly*, 2 декабря 2016 года, **http://www.computerweekly.com/news/450404018/UK-helps-dismantle-Avalanche-global-cyber-network**.

Вернуться

45

Самым печально известным примером такого рода была сеть, созданная Министерством государственной безопасности ГДР (*Штази*) в период между 1950 и 1990 годами. Штази вовлекло в нее более четверти миллиона граждан Восточной Германии, чтобы следить за всем населением страны и выявлять диссидентов.

Вернуться

46

Остановитесь на секунду и задумайтесь о том, сколько всего о вашей повседневной жизни могут знать мобильный телефон, поисковая система и социальные сети, собирая данные, которые вы генерируете

при взаимодействии с ними. Теперь представьте, насколько больше они могли бы о вас узнать, поделившись этой информацией друг с другом. Если хотите менее гипотетический пример, введите «наблюдение за работниками» в свою любимую поисковую систему (прибавив еще чуть-чуть к тем сведениям о вас, которые у нее уже есть). Результаты могут вас расстроить.

Вернуться

47

Криптография лежит в основе любого рода финансовых транзакций, включая те, которые мы проводим с банкоматами, дебетовыми и кредитными картами, а также с глобальной сетью SWIFT (Society for Worldwide Interbank Financial Telecommunications – Общество всемирных межбанковских финансовых каналов связи). Ежегодная конференция Financial Cryptography and Data Security, проводимая с 1997 года, посвящена теории и практике использования криптографии для защиты финансовых транзакций и созданию новых видов цифровых денег: Международная ассоциация по финансовой криптографии, **https://ifca.ai** (по состоянию на 10 июня 2019 года).

Вернуться

48

Следует признать, что рекомендательные письма в наши дни являются редкостью. Но мы все еще активно используем письменные рекомендации при собеседовании. Наша безопасность в материальном мире во многом основана на мнении других доверенных источников. Например, друг может представить нам человека, с которым мы раньше не были знакомы; в каком-то смысле это тоже устное «рекомендательное письмо».

Вернуться

49

Фраза «Сезам откройся» взята из сказки об «Али-Бабе и сорока разбойниках», входящей в *Книгу тысячи и одной ночи* – собрание народных сказок, которое, возможно, уходит корнями в восьмой век.
Вернуться

50

Заметьте, что в ASCII символ «9» является пятьдесят седьмым по счету, что может вызвать путаницу, так как он представлен в виде двоичного эквивалента числа 57, а не десятичного значения 9.
Вернуться

51

Длину ключа иногда называют *размером*. Я буду считать эти термины синонимами.
Вернуться

52

Количество абонентов мобильной связи в мире насчитывает более 5 миллиардов: «The Mobile Economy 2019», Ассоциация GSM, 2019 год, **https://www.gsma.com/mobileeconomy**.
Вернуться

53

Этот пример основан на предположении о том, что в нашей вселенной существует около 1022 звезд. Подсчет звезд – это не точная наука, так как мы можем только догадываться об их количестве по нашим наблюдениям с помощью существующих телескопов. По последним оценкам этот показатель приближается к 10^{24}, и многие специалисты подозревают, что он тоже может быть заниженным. Например, см. статью Элизабет Хауэлл, «How Many Stars Are in the

Universe?» от 18 мая 2017 года в разделе *Science & Astronomy* на сайте **https://www.space.com/26078-how-many-stars-are-there.html**. Подсчет криптографических ключей является куда более точным процессом!

Вернуться

54

Термин *персональный идентификационный номер* (англ. personal identification number или PIN) обычно используют для обозначения коротких паролей, состоящих из цифр. Он уходит своими корнями в конец 1960-х, когда появились первые банкоматы. В нашем контексте PIN-коды и пароли представляют собой одно и то же – строку секретных символов.

Вернуться

55

На самом деле в этом процессе нередко участвует криптография, поскольку компьютеры в большинстве своем хранят не копии ваших паролей, а значения, вычисленные на их основе с помощью криптографической функции особого типа.

Вернуться

56

При вводе PIN-кода в банкомат мы фактически надеемся на то, что он не сделает с ним ничего плохого. Однако существует много атак, известных как *скимминг*, в ходе которых преступники модифицируют банкомат, чтобы заполучить данные о карте и PIN-коде (последний можно узнать, наложив поддельную клавиатуру).

Вернуться

57

Один из способов, как этого можно достичь, состоит в использовании функции *PBKDF2*, описанной в предложении для обсуждения «PKCS #5: Password-Based Cryptography Specification Version 2.1»: 8018, Инженерный совет Интернета, январь 2017 года, **https://tools.ietf.org/html/rfc8018**.

Вернуться

58

Оксфордский словарь английского языка, Oxford Dictionaries, **https://languages.oup.com/oed** (по состоянию на 10 июня 2019 года).

Вернуться

59

Замечательным введением является книга Деборы Дж. Беннетт *Randomness* (Harvard University Press, 1998).

Вернуться

60

Действительно, одним из самых распространенных методов случайной генерации ключей для дальнейшего их использования в криптографических алгоритмах является использование (других) криптографических алгоритмов.

Вернуться

61

Типичное формальное требование к хорошему криптографическому алгоритму состоит в том, что между его выводом и результатами работы генератора случайных чисел не должно быть никакой видимой разницы.

Вернуться

62

Продукты для обеспечения безопасности, основанные на самопальных криптографических алгоритмах, относятся к категории, которую некоторые криптографы называют *snake oil* (бесполезное лекарство): Брюс Шнайер, «Snake Oil», *Crypto-Gram*, 15 февраля 1999 года, **https://www.schneier.com/crypto-gram/archives/1999/0215.html#snakeoil**.

Вернуться

63

Для сфер деятельности, которые не находятся в общественном доступе, это не совсем так. Правительственное агентство вполне может разработать секретный алгоритм для внутреннего использования при условии, что у этого агентства достаточно знаний и опыта в области криптографии.

Вернуться

64

За последние несколько десятилетий в публичной сфере произошел заметный сдвиг от секретных криптографических алгоритмов к открытым, чему поспособствовала разработка открытых криптографических стандартов.

Вернуться

65

Существует достаточно случаев раскрытия принципа действия секретных алгоритмов, применяемых в публичных технологиях. Одним из таких примеров является алгоритм шифрования A5/1, который используется в стандарте GSM (глобальной системе мобильной связи).

Вернуться

66

Аугуст Керхгофф, «La cryptographie militaire», *Journal des sciences militaires* 9 за январь и февраль 1883 года: 5–83 и 161–91. Английский перевод изложенных в этих статьях принципов можно найти на сайте Фабьена Птиколаса, Information Hiding Homepage: «Kerckhoffs' Principles from 'La cryptographie militaire'», **http://petitcolas.net/kerckhoffs** (по состоянию на 10 июня 2019 года).

Вернуться

67

Алгоритмы шифрования, которые использовались для защиты средств связи, были частью стандарта GSM 1990 года и хранились в тайне, но в более новых спецификациях, таких как стандарт LTE (Long-Term Evolution – долговременное развитие), вышедшего в 2008 году, они описаны публично.

Вернуться

68

Похоже, что ингредиент Merchandise 7X по-прежнему остается в тайне, несмотря на заявления о противоположном: Уильям Паундстоун, Big Secrets (William Morrow, 1985).

Вернуться

69

Конфиденциальность нужна всем, так как всем есть что скрывать. Часто можно услышать мантру о том, что людям, которым нечего скрывать, можно не беспокоиться о правительственных программах слежения. Ошибочность этого аргумента подробно раскрывается в книгах Дэниела Дж. Солова *Nothing to Hide* (Yale University Press,

2011) и Дэвида Лайона *Surveillance Studies: An Overview* (Polity Press, 2007).

Вернуться

70

Эрик Хьюз, *A Cypherpunk's Manifesto*, 9 марта 1993 года, **https://www.activism.net/cypherpunk/manifesto.html**.

Вернуться

71

Я использую фразу «не следует полностью доверять», чтобы вы относились к устройствам и сетям с осторожностью, и вовсе не пытаюсь вызвать у вас паранойю из-за полного отсутствия безопасности. Суть в том, что мы никогда не знаем наверняка, скомпрометированы ли наши устройства и сети каким-либо образом (например, путем установки вредоносного ПО), поэтому, чтобы проявить благоразумие, к ним всегда нужно относиться с определенной настороженностью.

Вернуться

72

Это, несомненно, спорный аргумент. Метаданные, связанные с тем, кому и как часто мы звоним, могут прийтись очень кстати следователям, у которых нет доступа к содержанию звонков. Полезность таких метаданных была проиллюстрирована в одном из документов, опубликованных Сноуденом, который касался сбора метаданных американского оператора телекоммуникационных услуг Verizon со стороны АНБ: Гленн Гринвальд, «NSA Collecting Phone Records of Millions of Verizon Customers Daily», *Guardian*, 6 июня 2013 года, **https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order**.

Вернуться

73

Хорошим введением в стеганографию является книга Питера Уэйнера *Disappearing Cryptography: Information Hiding: Steganography & Watermarking* (MK/Morgan Kaufmann, 2009).

Вернуться

74

С реальными примерами использования стеганографии для взлома компьютеров можно познакомиться в статье Бена Росси «How Cyber Criminals Are Using Hidden Messages in Image Files to Infect Your Computer» от 27 июля 2015 года, *Information Age*, **http://www.information-age.com/how-cyber-criminals-are-using-hidden-messages-image-files-infect-your-computer-123459881**.

Вернуться

75

Такого рода способы применения часто обсуждаются, и советы на этот счет можно легко найти в Интернете (например, Krintoxi, «Using Steganography and Cryptography to Bypass Censorship in Third World Countries», *Cybrary*, 5 сентября 2015 года, **https://www.cybrary.it/0p3n/steganography-and-cryptography-to-bypass-censorship-in-third-world-countries**), свидетельств его широкого распространения не так уж много. Причины этого, наверное, аналогичны тем, которые приводятся критиками утверждений о том, что стеганография активно использовалась террористами (которые стали звучать после событий 11 сентября 2001 года): Роберт Дж. Бэгнелл, «Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools», SANS Institute, 2002 год, **https://www.sans.org/reading-room/whitepapers/stenganography/reversing-steganography-myth-terrorist-operations-asymmetrical-threat-simple-intellig-556**. На самом

деле с тех пор, как Бэгнелл дал свои комментарии в 2002 году, и особенно с момента публикации разоблачений Сноудена в 2013 году, спектр средств безопасной связи, доступных любому, кто хочет избежать слежки со стороны правительства, расширился.

Вернуться

76

Шифр Атбаш – это древний способ кодирования букв в иврите (название *Атбаш* получено из первой и последней букв в еврейском алфавите). Высказываются мнения о том, что он применяется в нескольких местах библейской книги пророка Иеремии: Пол Хоскиссон, «Jeremiah's Game», *Insight* 30, no. 1 (2010): 3–4, **https://publications.mi.byu.edu/publications/insights/30/1/S00001-30–1.pdf**.

Вернуться

77

С краткой историей и спецификацией азбуки Морзе можно познакомиться в Британской энциклопедии, статья под заголовком «Morse Code», **https://www.britannica.com/topic/Morse-Code** (по состоянию на 21 июля 2019 года).

Вернуться

78

С историей расшифровки египетских иероглифов можно познакомиться в книге Эндрю Робинсона *Cracking the Egyptian Code: The Revolutionary Life of JeanFrançois Champollion* (Thames and Hudson, 2012).

Вернуться

79

Дэн Браун, *The Da Vinci Code* (Doubleday, 2003).
Вернуться

80

Большинство современных средств шифрования сопровождается отдельной криптографической проверкой, которая позволяет получателю узнавать, был ли шифротекст каким-либо образом модифицирован. Эти два процесса все чаще объединяются посредством использования алгоритмов аутентифицированного шифрования.
Вернуться

81

Мой коллега-криптограф Стивен Гэлбрейт совершенно не согласен. Он утверждает, что Тьюринг был достаточно умен и что в случае, если бы ему предложили идею об асимметричном шифровании, он бы, скорее всего, ответил: «Да, конечно!»
Вернуться

82

Названный в честь Блеза де Виженера, этот алгоритм шифрования был изобретен Джованни Баттистой Белласо в 1553 году. В то время шифр Виженера считался «невзламываемым», но расшифровать его относительно легко, если установить длину ключа – это можно сделать с помощью статистического анализа шифротекста. Хорошее объяснение как самого алгоритма, так и способа его взлома можно найти в книге Саймона Сингха *The Code Book* (Fourth Estate, 1999).
Вернуться

83

Подробней об истории и взломе машин Энигма можно почитать, к примеру, в книге Хью Себага-Монтефиоре *Enigma: The Battle for the Code* (Weidenfeld & Nicolson, 2004).

Вернуться

84

«Data Encryption Standard (DES)», Федеральные стандарты обработки информации (англ. Federal Information Processing Standards или FIPS), выпуск 46, январь 1977 года. Впоследствии этот стандарт был несколько раз пересмотрен и в итоге аннулирован в 2005 году. Последняя обновленная версия, выпуск 46–3, доступна в архиве по адресу: **https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999–10-25/documents/fips46–3.pdf**.

Вернуться

85

Triple DES фактически использует алгоритм DES три раза: сначала данные шифруются одним ключом, затем расшифровываются вторым, после чего результат снова шифруется третьим ключом (расшифровка в Triple DES повторяет этот процесс в обратном порядке). Изначально Triple DES был исправлением для DES, сделанным «на скорую руку», но он по-прежнему используется во многих приложениях, в частности в финансовом секторе. Подробности и рекомендации о применении Triple DES можно найти в документе «Recommendation for the Triple Data Encryption Standard (TDEA) Block Cipher», Илэйн Баркер и Ники Моуха, Национальный институт стандартов и технологий, NIST Special Publication 800–67, rev. 2, ноябрь 2017 года, **https://doi.org/10.6028/NIST.SP.800–67r2**.

Вернуться

86

«Specification for the Advanced Encryption Standard (AES)», Федеральные стандарты обработки информации, выпуск 197, 26 ноября 2001 года, **https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf**.

Вернуться

87

Краткий экскурс в историю принятия AES, включая связанную с этим документацию, можно найти в статье «AES Development», NIST Computer Security Resource Center, **https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development** (обновлено 10 октября 2018 года).

Вернуться

88

Все операции AES проводятся с квадратной матрицей байтов – неслучайно исходный алгоритм шифрования, на основе которого был разработан AES, назывался *Square* (квадрат).

Вернуться

89

Процесс разработки AES длился почти четыре года, и в итоге после интенсивной процедуры оценивания, состоявшей из трех специальных конференций, из пятнадцати претендентов был выбран один. Все подробности этого конкурса задокументированы в книге Джоан Дэмен и Винсента Рэймена *The Design of Rijndael* (Springer, 2002).

Вернуться

90

Здесь в том числе имеются в виду блочные шифры, включая *BEAR, Blowfish, Cobra, Crab, FROG, Grand Cru, LION, LOKI, Red Pike, Serpent, SHARK, Skipjack, Twofish* и *Threefish*.

Вернуться

91

NIST предлагает список некоторых рекомендованных режимов работы, в том числе только для конфиденциальности (CBC, CFB, ECB, OFB), только для аутентификации (CMAC), для аутентифицированного шифрования (CCM, GCM), для шифрования диска (XTS) и для защиты криптографических ключей (KW, KWP): «Block Cipher Techniques – Current Modes», NIST Computer Security Resource Center, **https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Current-Modes** (обновлено 17 мая 2019 года).

Вернуться

92

Это не совсем дилемма о курице и яйце, поскольку закрытый ключ можно передавать не только посредством шифрования. Однако шифрование является самым очевидным способом, который часто используется на практике.

Вернуться

93

Безопасность сетей Wi-Fi имеет несколько пеструю историю. Основные стандарты безопасности описаны в спецификациях серии IEEE 802.11. Они фактически ограничивают доступ к авторизованным устройствам и делают возможным шифрование взаимодействия по сети Wi-Fi. Другие связанные с этим стандарты, такие как WPS (Wi-Fi Protected Setup – защищенная установка), предназначены для упрощения инициализации ключей в беспроводных сетях.

Вернуться

94

«Total Number of Websites», Internet Live Stats, **http://www.internetlivestats.com/total-number-of-websites** (по состоянию на 10 июня 2019 года).

Вернуться

95

Распространение ключей с помощью доверенного центра может хорошо работать в централизованном окружении с очевидными точками доверия. Таким образом, к примеру, работает система сетевой аутентификации Kerberos: Kerberos: The Network Authentication Protocol», MIT Kerberos, **https://web.mit.edu/kerberos** (обновлено 9 января 2019 года).

Вернуться

96

В Интернете есть много хороших видеороликов о последующем процессе использования навесных замков для обмена секретными данными, например, Крис Бишоп, «Key Exchange», YouTube, 9 июня 2009 года, **https://www.youtube.com/watch?v=U62S8SchxX4**.

Вернуться

97

Функцию, которая подходит для асимметричного шифрования, иногда называют *односторонней функцией с потайным входом*. «Односторонняя» она потому, что ее вычисление должно быть простым, а обратное выполнение – сложным. «Потайной вход» указывает на то, что у настоящего получателя должна быть возможность обратить этот процесс (потайным входом выступает знание закрытого ключа расшифровки).

Вернуться

98

Теория сложности вычислений занимается классификацией вычислительных задач в зависимости от того, насколько сложно их выполнить. Отношениям между вычислительной сложностью и криптографией посвящен хороший учебник авторства Джона Толбота и Доминика Уэлша, *Complexity and Cryptography: An Introduction* (Cambridge University Press, 2006).

Вернуться

99

История изучения простых множителей, их важная роль в математике и другие области исследований обсуждаются в книге

Маркуса дю Сотоя *The Music of the Primes: Why an Unsolved Problem in Mathematics Matters* (HarperPerennial, 2004).

Вернуться

100

Рон Ривест, Ади Шамир и Лен Адлеман, «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems», *Communications of the ACM* 21, № 2 (1978): 120–26.

Вернуться

101

100 петафлопс = 100 000 000 000 000 000 операций в секунду.

Вернуться

102

Периодически обновляемый список самых быстрых суперкомпьютеров в мире, «TOP500 Lists», TOP500.org, **https://www.top500.org/lists/top500** (по состоянию на 21 июля 2019 года).

Вернуться

103

23 189 – это 2587-е по счету простое число. Если вы сомневаетесь, но не хотите проверять сами, советую посетить страницу «The Nth Prime Page» Эндрю Букера, **https://primes.utm.edu/nthprime** (по состоянию на 10 июня 2019 года).

Вернуться

104

Согласно рекомендациям NIST, для данных, которые нуждаются в защите до 2030 года, следует использовать произведение двух простых чисел длиной больше 3000 бит (см. «Recommendation for Key Management», Национальный институт стандартов и технологий, NIST Special Publication 800 Part 1, rev. 4, 2016). Такое число состоит из более чем 900 десятичных цифр, и RSA использует простые множители примерно того же размера; это означает, что каждое из простых чисел имеет длину более 450 десятичных цифр.

Вернуться

105

Чтобы понять, как работает RSA, достаточно знать основы модульной арифметики и теорему Эйлера – и то и другое должно быть знакомо всем, кто изучал введение в теорию чисел. Минимальные знания математики, которые для этого необходимы, можно также получить во многих учебниках по криптографии для начинающих, включая *Everyday Cryptography*, 2-е издание (Oxford University Press, 2017), Кейт М. Мартин.

Вернуться

106

Это замечание является сочетанием факта и немного шутливого предположения. Факт относится ко времени, которое требуется для получения множителей числа такого размера на традиционном компьютере. Считается, что эта операция длится примерно столько же, сколько поиск 128-битного ключа, что, как вы узнаете позже, требует около 50 миллионов миллиардов лет. Предположение, конечно же, состоит в том, что человечество может к тому времени вымереть. Считается, что наш вид существует на протяжении примерно 300 000 лет, поэтому такие далеко идущие прогнозы являются лишь догадками. Спектр возможных путей, которыми может пойти человечество в будущем, обсуждается в статье Джолин Крейтон «How Long Will [It] Take Humans to Evolve? What Will We Evolve Into?», *Futurism*, 12

декабря 2013 года, **https://futurism.com/how-long-will-take-humans-to-evolve-what-will-we-evolve-into**.

Вернуться

107

Таблицу, в которой блочные шифры разделены на категории в зависимости от того, насколько часто они используются (часто, нечасто и др.) можно найти внизу страницы «Block Cipher» на Википедии, **https://en.wikipedia.org/wiki/Block_cipher** (по состоянию на 10 июня 2019 года).

Вернуться

108

В ответ на угрозу, которую представляют квантовые компьютеры (мы обсудим ее позже), возникла крупная международная инициатива по поиску новых алгоритмов асимметричного шифрования, основанных на новых сложных задачах: «Post-quantum Cryptography», NIST Computer Security Resource Center, **https://csrc.nist.gov/Projects/Post-Quantum-Cryptography** (обновлено 3 июня 2019 года). Однако даже в рамках этого процесса рассматривается всего несколько принципиально разных задач, на которых основаны предложенные алгоритмы.

Вернуться

109

Асимметричное шифрование (с открытым ключом) имеет увлекательную историю развития. Его открытие в настоящее время приписывают исследователям из GCHQ, которые пытались решить проблему распространения закрытых ключей по сети. Принципиальная идея, легшая в основу асимметричного шифрования, была изложена Джеймсом Эллисом в 1969 году, хотя конкретный метод ее применения был описан в 1973 году Клиффордом Коксом. Но

только в 1997 году эти открытия стали доступны общественности. А тем временем похожий процесс происходил в публичной сфере; в 1976 году Уитфилд Диффи и Мартин Хеллман разработали аналогичную концепцию, конкретное воплощение которой впоследствии было предложено целым рядом исследователей. Среди них были Ривест, Шамир и Адлеман со своим алгоритмом RSA, сформулированным в 1977 году. Подробности ищите в статьях «The History of Non-secret Encryption», Cryptologia 23, № 3 (1999): 267–73 Джеймса Эллиса и «New Directions in Cryptography», *IEEE Transactions on Information Theory* 22, № 6 (1976): 644–54 Уитфилда Диффи и Мартина Хеллмана, а также в книге Стивена Леви *Crypto: Secrecy and Privacy in the New Cold War* (Penguin, 2000).

Вернуться

110

Многие считают, что задачи разложения на простые множители и поиска дискретных логарифмов по модульным числам являются одинаково сложными, однако алгоритмы асимметричного шифрования на основе эллиптических кривых имеют одно преимущество: поиск дискретного логарифма по эллиптическим кривым считается на порядок сложнее, что позволяет использовать более короткие ключи по сравнению с RSA. Для тех, кто изучал математику, понимание эллиптических кривых не составит труда, хотя в целом это область не для слабонервных. Все, что вам нужно знать, описывается в большинстве вводных материалов, посвященных математической стороне криптографии; например, см. Дуглас Р. Стинсон и Маура Б. Патерсон, *Cryptography: Theory and Practice*, 4-е издание. (CRC Press, 2018).

Вернуться

111

Хорошо задокументированный пример этой проблемы относится к атаке, в ходе которой 300 000 иранских граждан, уверенных в том, что они взаимодействуют с серверами Google Gmail, на самом деле

получили альтернативные открытые ключи, которые подключили их к поддельному сайту, использовавшемуся впоследствии для отслеживания их переписки. Эта атака произошла из-за того, что компания под названием DigiNotar, занимавшаяся сертификацией, была взломана, что позволило создать открытые ключи, которые ввели в заблуждение иранских пользователей Gmail. См. Грегг Кейзер, «Hackers Spied on 300,000 Iranians Using Fake Google Certificate», *Computerworld*, 6 сентября 2011 года, **https://www.computerworld.com/article/2510951/cybercrime-hacking/hackers-spied-on-300–000-iranians-using-fake-google-certificate.html**.

Вернуться

112

Культовый роман Лори Ли *Сидр с Рози* (Hogarth Press, 1959) основан на его детских воспоминаниях из 1920-х годов и описывает жизнь в маленькой английской деревне до появления таких прорывных технологий, как легковой автомобиль. Эта книга отражает, по всей видимости, утерянную провинциальную идиллию, свободную от суеты и связей с внешним миром.

Вернуться

113

В число примеров важных интернет-стандартов, каждый из которых использует гибридное шифрование, входят *TLS* (Transport Layer Security – протокол защиты транспортного уровня) для защиты веб-соединений, *IPSec* (Internet Protocol Security) для создания виртуальных частных сетей, позволяющих заниматься такими видами деятельности как удаленная работа, *SSH* (Secure Shell – безопасная оболочка) для безопасной передачи файлов и *S/MIME* (Secure Multipurpose Internet Mail Extensions) для защиты электронной почты.

Вернуться

114

Исследовательско-консалтинговая компания Gartner известна своей простой методологией под названием *цикл хайпа* для отслеживания ожиданий относительно новых технологий (см. «Gartner Hype Cycle», Gartner, **https://www.gartner.com/en/research/methodologies/gartner-hype-cycle** [по состоянию на 10 июня 2019 года]). Этот цикл характеризуется ранним пиком завышенного и зачастую плохо информированного ажиотажа, затем стремительным падением, связанным с выявлением сложностей реализации, за которым следует плавный подъем, когда становятся понятными реальные сферы применения технологии. Асимметричное шифрование, вероятно, дошло до «плато продуктивности»: всем уже понятны его плюсы и минусы, и теперь его можно использовать по назначению.

Вернуться

115

Исследования в области когнитивной психологии показывают, что большинство людей предпочло бы избежать потерь, нежели получить прибыль того же размера. Эта *боязнь потерь* стала одним из ряда искажений восприятия, которые популяризировал Дэниел Канеман в книге *Thinking Fast and Slow* (Penguin, 2012).

Вернуться

116

Заметьте, что целостность данных заключается лишь в обнаружении ошибок, но не в их исправлении. Отдельные математические методики, известные как *контроль ошибок*, позволяют в какой-то степени автоматизировать процесс исправления. Эти методики обычно не относят к безопасности и используют там, где ожидается появление ошибок, о существовании которых мы не хотим знать, например при воспроизведении цифровой музыки.

Вернуться

117

Вплоть до середины 1980-х годов шахтеры в Великобритании и других странах использовали канареек в клетках для обнаружения токсичных газов. На смену этому методу пришли цифровые датчики: Кэт Эшнер, «The Story of the Real Canary in the Coal Mine», *Smithsonian*, 30 декабря 2016 года, **https://www.smithsonianmag.com/smart-news/story-real-canary-coal-mine-180961570**.

Вернуться

118

Термин *фейковые новости* (от англ. fake news) часто ассоциируют с Дональдом Трампом, который с его помощью характеризовал отрицательное освещение в прессе своей предвыборной кампании на президентских выборах. Однако намеренное распространение информации (как достоверной, так и нет) – это древнее ремесло. В нашем контексте важно то, что цифровые СМИ этот процесс упрощают и ускоряют.

Вернуться

119

Есть основания полагать, что людям сложнее распознавать фейковые новости, которые распространяются через цифровые СМИ: Саймон Йейтс, «‘Fake New People Believe It and What Can Be Done to Counter It», *Conversation*, 13 декабря 2016 года, **https://theconversation.com/fake-news-why-people-believe-it-and-what-can-be-done-to-counter-it-70013**.

Вернуться

120

«Integrity», Lexico, **https://www.lexico.com/en/definition/integrity** (по состоянию на 12 июня 2019 года).

Вернуться

121

Примечательно, что доверие в таких отношениях быстро угасает. Если вы доверяете своему другу Чарли, а тот верит своей подруге Диане, то в какой степени Диана заслуживает вашего доверия? Возможно, вы поверите ей в чем-то одном, но вряд ли вы станете доверять всем ее друзьям; эти связи быстро становятся довольно хрупкими. И чем дальше, тем меньше доверия у вас остается. Это имеет потенциальные последствия в киберпространстве, где, скажем, активные пользователи социальных сетей могут быстро собрать целую армию предполагаемых «друзей».

Вернуться

122

MD5 – это криптографическая хеш-функция, разработанная Рональдом Ривестом (ему принадлежит «R» в RSA) в 1991 году. Значение, которое она возвращает, имеет длину 128 бит. Ее полная спецификация описана в предложении для обсуждения 1321, «The MD5 Message-Digest Algorithm»: Инженерный совет Интернета, апрель 1992 года, **https://tools.ietf.org/html/rfc1321**. Стоит отметить, что впоследствии в MD5 были обнаружены серьезные уязвимости; см. «Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms», предложении для обсуждения 6151: Инженерный совет Интернета, март 2011, **https://tools.ietf.org/html/rfc6151**.

Вернуться

123

Печати для этого используются столько, сколько существует сама цивилизация. Например, древние каменные печати для создания углублений в глине являются для историков важными археологическими объектами: Марта Амери и др., *Seals and Sealing in the Ancient World* (Cambridge University Press, 2018).

Вернуться

124

Номер ISBN впервые был разработан в 1970 году. Его современная версия состоит из тринадцати цифр, включая идентификаторы для страны происхождения и издателя книги. Чтобы узнать все подробности о книге, ISBN можно ввести на сайте ISBN Search, **https://isbnsearch.org** (по состоянию на 10 июня 2019 года).

Вернуться

125

В большинстве этих примеров используется алгоритм, названный в честь Ганса Петера Луна, который запатентовал его в 1960 году. Алгоритм Луна для вычисления контрольной цифры похож на тот, который используется в ISBN, но имеет некоторые отличия: Википедия, «Luhn Algorithm», **https://ru.wikipedia.org/wiki/Алгоритм_Луна**.

Вернуться

126

Интересно, что термин *хеш-функция* используется в области компьютерных наук для нескольких разных целей. Я ограничусь только одним его значением, которое относится к так называемым *криптографическим хеш-функциям*.

Вернуться

127

Ранее я упоминал хеш-функцию MD5, которая часто используется для проверки целостности загруженных файлов. В качестве других примеров хеш-функций, которые применяются на практике, можно привести *SHA-1, семейство SHA-2* и *семейство SHA-3*; в 2015 году последнее стало победителем международного конкурса, который проводился Национальным институтом стандартов и технологий США: «Hash Functions», NIST Computer Security Resource Center, **https://csrc.nist.gov/Projects/Hash-Functions** (обновлено 3 мая 2019 года).

Вернуться

128

Проблема не в самой идее, а в архитектуре многих хеш-функций. Грубо говоря, хеш-функции нередко принимают какие-то данные, сжимают их, принимают еще немного, сжимают и т. д. Таким образом, если добавить ключ в конец, он не смешается с данными настолько хорошо, насколько это возможно.

Вернуться

129

«HMAC: Keyed-Hashing for Message Authentication», предложение для обсуждения 2104: Инженерный совет Интернета, февраль 1997 года, **https://tools.ietf.org/html/rfc2104**.

Вернуться

130

«The AES-CMAC Algorithm», предложение для обсуждения 4493: Инженерный совет Интернета, июнь 2006 года, **https://tools.ietf.org/html/rfc4493**.

Вернуться

131

Существует множество разных причин, почему режимы аутентифицированного шифрования, которые объединяют в себе шифрование и вычисление имитовставки, превосходят методы, где эти два этапа разделены. Некоторые из этих причин связаны с эффективностью, но большинство из них относятся к безопасности. В сущности, при выполнении этих двух операций по отдельности кое-что может пойти не так, и этих проблем можно избежать, если использовать одобренный режим аутентифицированного шифрования. Примерами таких режимов являются *CCM* («Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality», NIST Special Publication 800–38C, 20 июля 2007 года) и *GCM* («Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode [GCM] and GMAC», NIST Special Publication 800–38D, ноябрь 2007 года).

Вернуться

132

Этот аргумент не предполагает никаких дополнительных доказательств вроде журнальной записи в защищенной сети, которая явно доказывает, что имитовставка была передана по сети с тем же интернет-адресом, что и у отправителя.

Вернуться

133

Цифровые подписи тоже были бы небезопасными. Если вы хотите подписать очень длинный документ, вам нужно разбить его на отдельные блоки данных, каждый из которых должен получить свою подпись. Злоумышленник может перехватить эту цепочку отдельных блоков вместе с сопутствующими подписями и поменять их местами.

В результате получится корректный набор подписанных блоков данных. Но, если объединить их в сообщение, окажется, что они неправильно упорядочены.

Вернуться

134

Подписи, которые ставят от руки, являются на удивление долговечными и используются повсеместно, что свидетельствует об их удобстве. Несмотря на все более широкое применение цифровых документов, подписи, поставленные от руки, по-прежнему преобладают благодаря общепринятой практике их сканирования. Цифровая копия традиционной подписи представляет собой небольшой файл с изображением, который легко извлечь из документа; в этом отношении она является еще более слабым механизмом, чем оригинальная подпись, поставленная от руки.

Вернуться

135

Организация *Репортеры без границ* публикует «*Индекс свободы прессы*», основанный на анализе независимости, самоцензуры, законодательства, прозрачности и качества инфраструктуры СМИ. Северная Корея, где прослушивание или просмотр заграничного медиа-контента считается преступлением, неизменно находится в нижней части таблицы: «North Korea», Репортеры без границ, **https://rsf.org/en/north-korea** (по состоянию на 10 июня 2019 года).

Вернуться

136

Внимание общественности к этой идее привлекла книга Эли Паризера *The Filter Bubble* (Penguin, 2012).

Вернуться

137

По моему опыту, качество информации на Википедии, относящейся к криптографии, довольно неплохое. Это свидетельствует как о значительном интересе к криптографии среди пользователей Интернета, так и, пожалуй, о том, что люди, интересующиеся криптографией, нередко имеют желание (и/или возможность) редактировать страницы на Википедии.

Вернуться

138

Когда теряется доверие к банку, деньги, естественно, уходят в другое место. Это, например, произошло в 2007 году во время краха Британского банка Northern Rock: Доминик О'Коннелл, «The Collapse of Northern Rock: Ten Years On», BBC, 12 сентября 2017 года, **https://www.bbc.co.uk/news/business-41229513**.

Вернуться

139

О Bitcoin существует множество информации. Доминик Фрисби написал замечательную книгу о необходимости (и использовании) Bitcoin, *Bitcoin: The Future of Money?* (Unbound, 2015). Удобочитаемое введение в криптографию, которая применяется в Bitcoin, написал Андреас М. Антонопулос, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly, 2014).

Вернуться

140

Существует много примеров того, как некоторые аспекты цифровых денег пытались реализовать в рамках централизованной банковской системы. Это в том числе относится к технологиям цифрового

кошелька, разработанным в 1990-х годах, таким как Mondex и Proton, и более современным системам вроде Apple Pay. Предоставляя некоторые удобные возможности, присущие наличным деньгам, они, тем не менее, остаются привязанными к традиционным банковским счетам.

Вернуться

141

Банки стали пионерами коммерческого использования криптографии в 1970-х. Мотивация, стоявшая за созданием стандарта DES (Data Encryption Standard – стандарт шифрования данных), и его успех были во многом вызваны тем, что финансовый сектор нуждался в цифровой безопасности.

Вернуться

142

Одна из многих остроумных особенностей Bitcoin состоит в том, что у этой системы есть параметр, с помощью которого можно контролировать частоту создания блоков.

Вернуться

143

Прибыльность майнинга биткоинов, идущая немного вразрез с духом децентрализации этой системы, привела к появлению огромных вычислительных центров, предназначенных специально для этой цели. Их иногда называют *фермами*: Джулия Магас, «Top Five Biggest Crypto Mining Areas: Which Farms Are Pushing Forward the New Gold Rush?», Cointelegraph, 23 июня 2018 года, **https://cointelegraph.com/news/top-five-biggest-crypto-mining-areas-which-farms-are-pushing-forward-the-new-gold-rush**.

Вернуться

144

Это часто называют *форком* блокчейна (от англ. fork).
Вернуться

145

Полный список текущих криптовалют доступен на странице «Cryptocurrency List», CoinLore, **https://www.coinlore.com/all_coins** (по состоянию на 10 июня 2019 года).
Вернуться

146

Например, см. Майкл Кавна, «‘Nobody Knows You’re a Dog’: As Iconic Internet Cartoon Turns 20, Creator Peter Steiner Knows the Joke Rings as Relevant as Ever», *Washington Post*, 31 июля 2013 года.
Вернуться

147

Согласно отчету, предоставленному компанией Facebook (Сейчас Meta Platforms Inc. – организация, деятельность которой запрещена на территории Российской Федерации.) Комиссии по ценным бумагам и биржам США, в 2017 году каждый из ее 1,4 миллиарда пользователей принес прибыль в размере 20,21$: Джулия Глум, «This Is Exactly How Much Your Personal Information Is Worth to Facebook*», *Money*, 21 марта 2018 года, **http://money.com/money/5207924/how-much-facebook-makes-off-you**.
Вернуться

148

Если вас интересует обсуждение распространенных угроз для паспортов и методы защиты от них, можете почитать «Passport Security Features: 2019 Report Anatomy of a Secure Travel Document», Gemalto, **https://www.gemalto.com/govt/travel/passport-security-design** (обновлено 20 мая 2019 года).

Вернуться

149

Вот почему мы используем в наших телефонах различные механизмы безопасности. Сотовые операторы применяют эти механизмы на SIM-карте для идентификации абонента. Абонент, как правило, использует PIN-код или пароль для контроля доступа к своему телефону.

Вернуться

150

Теоретически для осуществления банковских махинаций на телефон можно установить шпионское ПО, однако чаще всего атаки на мобильный банкинг проводятся путем похищения телефонного номера или привязки других телефонных номеров к банковскому счету жертвы. Например, см. статьи Майлза Бригналла «Mobile Banking in the Spotlight as Fraudsters Pull £6,000 Sting», *Guardian*, 2 апреля 2016 года, **https://www.theguardian.com/money/2016/apr/02/mobile-banking-fraud-o2-nationwide** и Анны Тимс, «‘Sim Swap’ Gives Fraudsters Access-All-Areas via Your Mobile Phone», *Guardian*, 26 сентября 2015 года, **https://www.theguardian.com/money/2015/sep/26/sim-swap-fraud-mobile-phone-vodafone-customer**.

Вернуться

151

Алан Тьюринг придумал знаменитый тест, названный в его честь и предназначенный для того, чтобы отличить поведение компьютера от поведения человека: Алан М. Тьюринг, «Computing Machinery and Intelligence», *Mind* 59, № 236 (октябрь 1950 года): 433–60.

Вернуться

152

Такого рода вредоносное ПО часто называют *кейлоггером*. Познакомиться с этой темой можно в статье Николая Гребенникова «Keyloggers: How They Work and How to Detect Them», SecureList, 29 марта 2007 года, **https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138**.

Вернуться

153

Капчи пользуются дурной славой, так как они отнимают время и при их вводе можно легко ошибиться, что приводит к дополнительным задержкам. Обзор некоторых альтернативных подходов можно найти в статье Мэтта Берджесса «Captcha Is Dying. This Is How It's Being Reinvented for the AI Age», *Wired*, 26 октября 2017 года, **https://www.wired.co.uk/article/captcha-automation-broken-history-fix**.

Вернуться

154

Хорошим введением в биометрию является книга Джона Р. Вакки *Biometric Technologies and Verification Systems* (Butterworth-Heinemann, 2007).

Вернуться

155

Известным примером «похищения» биометрии являются так называемые *липкие пальцы* – это искусственные пальцы, созданные для обхода систем распознавания отпечатков: Цутому Мацумото и др., «Impact of Artificial 'Gummy' Fingers on Fingerprint Systems», *материалы к SPIE* 4677 (2002), **https://cryptome.org/gummy.htm**.

Вернуться

156

Банки могли бы подойти к делу более основательно, например, у каждого персонального устройства мог бы быть кардридер для считывания самих физических карт, а не только напечатанных на них данных. Но, как и с любыми мерами безопасности, это вопрос баланса между защищенностью, стоимостью и удобством использования.

Вернуться

157

Обзор мошенничества с непредъявлением банковских карт разной степени серьезности приводится в статье «Card-Not-Present Fraud around the World», US Payments Forum, март 2017 года, **https://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf**. Например, этот вид мошенничества составил 69 процентов от всех махинаций с банковскими картами в Великобритании за 2014 год и 76 процентов в Канаде за 2015 год.

Вернуться

158

Аутентификация и авторизация – это связанные между собой вещи, которые часто путают. Аутентификация в основном позволяет узнать, с кем мы имеем дело. Авторизация определяет, что этому человеку позволено делать. Когда вы входите в свою учетную запись в социальной сети, вы аутентифицируетесь. Затем социальная сеть

выполняет процесс авторизации, чтобы определить, какие данные вам можно просматривать. Авторизация часто следует за аутентификацией, но ее можно использовать отдельно. Работник в супермаркете авторизует продажу алкоголя, определяя возраст покупателя (иногда для этого достаточно взглянуть на человека, а иногда необходимо потребовать документы, подтверждающие возраст); при этом личность человека проверять не нужно. Криптография предоставляет инструменты для аутентификации, но этот процесс обычно выполняется другими средствами (например, с помощью правил, которые ограничивают доступ к записям в базе данных).

Вернуться

159

Этот подход больше не является надежным ввиду доступности мощных программных редакторов.

Вернуться

160

Из выступления Элизабет Стоберт, «The Agony of Passwords», на конференции *CHI ’14 Extended Abstracts on Human Factors in Computing Systems* (ACM, 2014), 975–80.

Вернуться

161

Советы об организации паролей зачастую противоречат друг другу. Это объясняется необходимостью поиска непростого компромисса. Например, регулярная замена паролей смягчает последствия от их раскрытия, но в то же время усложняет жизнь тем, кто эти пароли использует, подталкивая их к рискованным мерам, таким как запись паролей на листе бумаги. Общее руководство по работе с паролями, к примеру, приводится в статье «Password Administration for System Owners» от Центра национальной компьютерной безопасности

Великобритании за 19 ноября 2018 года, **https://www.ncsc.gov.uk/collection/passwords**.

Вернуться

162

Что еще хуже, помимо создания отдельной дыры в безопасности, такие атаки, судя по всему, накапливают огромные архивы похищенных паролей с сопутствующими учетными данными: Мохит Кумар, «Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online», *Hacker News*, 12 декабря 2017 года, **https://thehackernews.com/2017/12/data-breach-password-list.html**.

Вернуться

163

В 2019 году компания Facebook (Сейчас Meta Platforms Inc. – организация, деятельность которой запрещена на территории Российской Федерации.) признала, что в результате программной ошибки в ее системе управления паролями сотни миллионов пользовательских паролей хранились во внутренней платформе в незашифрованном виде: Лили Хэй Ньюман, «Facebook* Stored Millions of Passwords in Plaintext – Change Yours Now», *Wired*, 21 марта 2019 года, **https://www.wired.com/story/facebook-passwords-plaintext-change-yours**.

Вернуться

164

Советы о том, как выбрать устойчивый пароль, можно найти во многих источниках. Одним из примеров являются рекомендации от Национального института стандартов и технологий, которые собраны в статье Майка Гарсии «Easy Ways to Build a Better P@$5w0rd», NIST, *Taking Measure* (блог), 4 октября 2017 года,

https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

Вернуться

165

Такое отношение не ново. В 1980-х один мой коллега услышал следующее от системного инженера: «Криптография – это не более чем дорогой способ ухудшения производительности».

Вернуться

166

В число алгоритмов расширения ключа входят *PBKDF2* и *Argon2*.

Вернуться

167

Если вас интересует взгляд британского правительства на полезность менеджеров паролей, см. статью Эммы У. «What Does the NCSC Think of Password Managers?», Центр национальной компьютерной безопасности, 24 января 2017 года, **https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers**.

Вернуться

168

В отчете о расследовании утечек данных, составленном компанией Verizon в 2016 году, утверждается, что 63 процента подтвержденных утечек стали возможными благодаря паролям, которые либо плохо сгенерировали, либо забыли поменять (то есть использовался пароль по умолчанию), либо похитили. Самую свежую версию отчета Verizon можно загрузить на странице **https://www.verizonenterprise.com/verizon-insights-lab/dbir**.

Вернуться

169

Ряд примеров фишинга, а также советы о том, как обнаружить эти атаки и стать их жертвой, приводится на веб-сайте Phishing.org, **https://www.phishing.org** (по состоянию на 4 августа 2019 года).

Вернуться

170

Многое свидетельствует о том, что принудительная регулярная замена паролей может не дать желаемого результата: «Time to Rethink Mandatory Password Changes», Федеральная торговая комиссия, 2 марта 2016 года, **https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes**.

Вернуться

171

Токены аутентификации для интернет-банкинга остаются в широком употреблении, но это относительно дорогой подход. В качестве альтернативного решения можно использовать уже имеющиеся у клиентов устройства, способные производить криптографические вычисления. Вот почему все больше банков поддерживает аутентификацию с помощью приложений для мобильных телефонов. Еще один метод состоит в использовании *ключей*, которые у клиентов уже есть; для этого некоторые банки выпускают кардридеры, способные считывать ключи на чипе банковской карты.

Вернуться

172

Алгоритмы с функцией прогнозирования можно использовать для отслеживания расхождения во времени между отдельно взятым

токеном и главными часами, на которых основана система. Когда клиент пытается аутентифицироваться, банк оценивает с помощью такого алгоритма время на часах его токена, учитывая предыдущие сеансы взаимодействия с ним. Банк также может считать приемлемым любое расхождение в каких-то небольших пределах.

Вернуться

173

Многочисленные атаки, получившие широкую огласку, были направлены на системы автомобильных ключей. Некоторые из них стали возможными из-за того, что автопроизводители использовали пароли по умолчанию для всех машин какого-то определенного типа. Но даже те из них, которые следовали принципам «идеальных паролей», пострадали от разных вариантов *релейных атак*, в ходе которых злоумышленник со специальным радиоустройством занимает позицию между автомобилем (припаркованным у дома) и ключом (висящим в прихожей), инициируя взаимодействие между ними; например, см. статью Дэвида Биссона «Relay Attack against Keyless Vehicle Entry Systems Caught on Film», Tripwire, 29 ноября 2017 года, **https://www.tripwire.com/state-of-security/security-awareness/relay-attack-keyless-vehicle-entry-systems-caught-film**.

Вернуться

174

Не все бумеранги изготавливают так, чтобы они возвращались. В этом примере с охотой бумеранг должен подлететь к уткам с обратной стороны и спугнуть их, чтобы они полетели к охотнику; следовательно, бумеранг может и не возвращаться обратно в руки. Неважно – я просто хотел привести аналогию! Ценителям бумерангов настоятельно советую почитать книгу Филипа Джонса *Boomerang: Behind an Australian Icon* (Wakefield Press, 2010).

Вернуться

175

Мелалеука пятижилковая — это дерево, изначально произраставшее в Юго-Восточной Азии и Австралии. Сейчас его высаживают по всему миру как в качестве декоративного растения, так и для осушения болот. Оно имеет цветки с ярко выраженным ароматом, который не всем по душе.

Вернуться

176

Похожий принцип лежит в основе *систем радиолокационного опознавания* («свой-чужой»), которые впервые были разработаны в 1930-х для определения того, является подлетающий самолет дружественным или вражеским. Если вам интересен исторический экскурс на эту тему, см. статью Лорда Боудена «The Story of IFF (Identification Friend or Foe)», *IEE Proceedings A (Physical Science, Measurement and Instrumentation, Management and Education, Reviews)* 132, № 6 (октябрь 1985 года): 435–37.

Вернуться

177

Спецификация самой новой версии TLS описана в предложении для обсуждения 8446 «The Transport Layer Security (TLS) Protocol Version 1.3»: Инженерный совет Интернета, август 2018, **https://tools.ietf.org/html/rfc8446**.

Вернуться

178

Аргумент о том, что анонимность является одним из основополагающих прав человека, приводится в статье Джиллиана Йорка «The Right to Anonymity Is a Matter of Privacy», Electronic

Frontier Foundation, 28 января 2012 года, **https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy**.

Вернуться

179

С разными примерами того, как поведение человека меняется в киберпространстве, можно познакомиться в книге Мэри Эйкен *The Cyber Effect* (John Murray, 2017).

Вернуться

180

Хорошим ресурсом с объяснением угроз, которые представляет такое поведение, а также способов борьбы с ними является вебсайт «Get Safe Onli Expert Advice», **https://www.getsafeonline.org** (по состоянию на 10 июня 2019 года).

Вернуться

181

Данные, которые мы оставляем в ходе нашей деятельности в киберпространстве, иногда называют *цифровым следом*. Чтобы как следует понять эту концепцию, можно ознакомиться с тем, как следователи пытаются воссоздать действия людей в киберпространстве, используя методы компьютерной криминалистики. Хорошим введением в эту область является книга Джона Сэммонса *The Basics of Digital Forensics* (Syngress, 2014).

Вернуться

182

Tor – это свободное программное обеспечение, доступное для загрузки на сайте **https://www.torproject.org**.

Вернуться

183

В своей книге *The Dark Net* (Windmill, 2015) Джейми Бартлетт проводит захватывающее расследование одних из самых злостных видов деятельности в киберпространстве, которые являются возможными благодаря анонимности.

Вернуться

184

Многие пионеры Интернета считали киберпространство новым миром, свободным от ограничений, сложившихся в обществе. Возможность сохранять анонимность в киберпространстве была ключом к воплощению этого видения. Это задокументировано в книге Томаса Рида *Rise of the Machines* (W. W. Norton, 2016).

Вернуться

185

Эндрю Лондон, «Elon Musk’s Neuralink – Everything You Need to Know», TechRadar, 19 октября 2017 года, **https://www.techradar.com/uk/news/neuralink**.

Вернуться

186

Даже если обрушение моста спишут на гайки и шурупы, причина, скорее всего, в том, что их неправильно использовали. Например, в 2016 году в Канаде обрушился мост, и причиной назвали перегрузку болтов, но не сами болты: Эмили Эшуэлл, «Overloaded Bolts Blamed for Bridge Bearing Failure», *New Civil Engineer*, 28 сентября 2016 года, **https://www.newcivilengineer.com/world-view/overloaded-bolts-blamed-for-bridge-bearing-failure/10012078.article**. Позже я расскажу о том, как неправильное применение криптографии может стать причиной взлома криптосистемы.

Вернуться

187

То, как Цезарь использовал шифрование, описано в труде Гая Светония Транквилла «Жизнь двенадцати цезарей». Перевод на английский язык доступен на веб-сайте Project Gutenberg, **https://www.gutenberg.org/files/6400/6400-h/6400-h.htm** (по состоянию на 10 июня 2019 года; см. «Caius Julius Caesar Clause 56»).

Вернуться

188

Подробней о шифре Марии Стюарт и заговоре Бабингтона с целью свержения Елизаветы I можно почитать в разделе «Mary, Queen of Scots (1542–1587)» Национальных архивов Великобритании,

http://www.nationalarchives.gov.uk/spies/ciphers/mary (по состоянию на 10 июня 2019 года). То, как Мария Стюарт применяла шифрования, также описывается в книге Саймона Сингха *The Code Book* (Fourth Estate, 1999).

Вернуться

189

Больше подробностей о замысловатом шпионском агентстве Елизаветы I можно найти в книге Роберта Хатчинсона *Elizabeth's Spy Master: Francis Walsingham and the Secret War That Saved England* (Weidenfeld & Nicolson, 2007).

Вернуться

190

Например, ISO/IEC 18033 – это составной стандарт, описывающий ряд алгоритмов шифрования: «ISO/IEC 18033 Information Technology – Security Techniques – Encryption Algorithms», Международная организация по стандартизации.

Вернуться

191

С годами Брюс Шнайер «разоблачил» длинный список некачественных криптографических продуктов, которые он называет «cryptographic snake oil». См. архивы его новостной рассылки *Crypto-Gram*: Schneier on Security, **https://www.schneier.com/crypto-gram** (по состоянию на 4 августа 2019 года).

Вернуться

192

Согласно Дональду Рамсфельду, «Сообщения, в которых говорится о том, что чего-то не произошло, всегда интересны для меня, потому

что, как мы знаем, есть известные знания (known knowns): есть вещи, про которые мы знаем, что мы знаем. Мы также знаем, что есть известное незнание, то есть мы знаем, что некоторые вещи мы знаем. Но есть и неизвестное незнание – вещи, о которых мы не знаем, что мы не знаем. И, если взглянуть на историю нашей страны и других свободных стран, именно последняя категория обычно вызывает трудности». Полная стенограмма пресс-конференции Дональда Рамсфельда доступна на странице «DoD News Briefing – Secretary Rumsfeld and Gen. Myers», 12 февраля 2002 года, **http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636**.

Вернуться

193

АНБ, по всей видимости, ограничило длину ключа DES, но считается, что при этом оно усилило сам алгоритм, сделав его устойчивей к атакам, известным как *дифференциальный криптоанализ*. Сообществу гражданских исследователей это удалось обнаружить только в 1980-х. Например, см. Питер Брайт, «The NSA's Work to Make Crypto Worse and Better», Ars Technica, 9 июня 2013 года, **https://arstechnica.com/information-technology/2013/09/the-nsas-work-to-make-crypto-worse-and-better**; если вас интересуют подробности, см. статью Дона Копперсмита «The Data Encryption Standard (DES) and Its Strength against Attacks», *IBM Journal of Research and Development* 38, № 3 (1994): 243–50.

Вернуться

194

Это следует из того факта, что стороны обладают разными возможностями. В разведывательных службах работает много криптографов, и у них есть доступ ко всему, что публикуется открыто. Однако сами эти службы редко делятся своими знаниями, поэтому информации о криптографии у них должно быть больше. Вопрос в

том, знают ли они что-то важное, о чем не известно широкой общественности? И откуда бы мы бы об этом с вами узнали?

Вернуться

195

Самым знаменитым методом предсказания вычислительных мощностей является закон Мура. Гордон Мур из Intel предложил эмпирический принцип, согласно которому количество компонентов на интегральной схеме удваивается примерно раз в два года. На протяжении нескольких десятилетий эта оценка была довольно точной, однако на сегодня она уже не кажется самым мерилом будущего прогресса: М. Митчелл Уолдроп, «The Chips Are Down for Moore's Law», *Nature*, 9 февраля 2016 года, **https://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338**.

Вернуться

196

Сяоюнь Ванг и др., «Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD», Cryptology ePrint Archive 2004/199, вер. от 17 августа 2004 года, **https://eprint.iacr.org/2004/199.pdf**.

Вернуться

197

Интересно, что машина, способная расшифровывать данные без знания алгоритма, фигурирует в романе Дэна Брауна *Digital Fortress* (St. Martin's Press, 1998).

Вернуться

198

Поиск ключей методом полного перебора иногда называют *атакой методом «грубой силы»* (от англ. brute force).

Вернуться

199

Эти грубые расчеты основаны на анализе, похожем на тот, который приводится в статье Мохита Ароры «How Secure Is AES against Brute Force Attacks?», *EE Times*, 7 мая 2012 года, **https://www.eetimes.com/document.asp?doc_id=1279619**.

Вернуться

200

Эта оценка взята из публикации Уитфилда Диффи и Мартина Хеллмана «Exhaustive Cryptanalysis of the NBS Data Encryption Standard», *Computer* 10 (1977): 74–84.

Вернуться

201

Проект DESCHALL стал первым победителем ряда конкурсов, организованных компанией кибербезопасности RSA Security в 1997 году, и выиграл приз в размере $10 000 за успешное нахождение ключа DES методом полного перебора. Подробная история об этом проекте изложена в книге Мэтта Кертина *Brute Force* (Copernicus, 2005).

Вернуться

202

См. Сара Джордано, «Napoleon’s Guide to Improperly Using Cryptography», *Cryptography: The History and Mathematics of Codes and Code Breaking* (блог), **http://derekbruff.org/blogs/fywscrypto** (по состоянию на 10 июня 2019 года).

Вернуться

203

О криптоанализе машин Энигма написано немало. Одним из самых подробных и авторитетных источников является книга Владислава Козачука *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two* (Praeger, 1984).

Вернуться

204

Эти методики включают шифрование каждого блока исходного текста вместе с счетчиком, который инкрементируется на каждом этапе, а также шифрование каждого блока исходного текста вместе с предыдущим зашифрованным блоком (который, в сущности, является случайным числом). См. «Block Cipher TechniquesCurrent Modes», NIST Computer Security Resource Center, 17 мая 2019 года, **https://csrc.nist.gov/Projects/Block-Cipher-Techniques/BCM/Current-Modes**.

Вернуться

205

Копию этой записки можно найти в разделе «The Babington Plot», Secrets and Spies, Национальных архивов Великобритании, **http://www.nationalarchives.gov.uk/spies/ciphers/mary/ma2.htm** (по состоянию на 10 июня 2019 года).

Вернуться

206

Некоторые фишинговые атаки работают именно так, подсовывая вам с виду безопасную ссылку на веб-сайт, адрес которого очень похож на настоящий (например, на адрес банка), но на самом деле он принадлежит злоумышленнику. Таким образом, используя TLS-

соединение, злоумышленник защищает данные, которые вы по ошибке передали поддельному веб-сайту, от других злоумышленников!

Вернуться

207

Шифр RC4 больше не считается достаточно безопасным для применения криптографии в современных условиях: Джон Лейден, «Microsoft, Cisco: RC4 Encryption Considered Harmful, Avoid at All Costs», *Register*, 14 ноября 2013 года, **https://www.theregister.co.uk/2013/11/14/ms_moves_off_rc4**.

Вернуться

208

Подробности о криптографических уязвимостях в WEP находятся в широком доступе. Например, см. Кейт М. Мартин, *Everyday Cryptography*, 2-е издание (Oxford University Press, 2017), 488–95.

Вернуться

209

Протокол WEP для защиты Wi-Fi сначала был обновлен до протокола под названием WPA (Wi-Fi Protected Access), а затем до более безопасной версии WPA2, вышедшей в 2004 году и ставшей протоколом защиты Wi-Fi по умолчанию. В 2018 году было объявлено, что на смену WPA2 придет WPA3, хотя, как ожидается, внедрение этой новой версии займет много лет, так как во многих случаях переход на этот протокол состоится только при замене оборудования.

Вернуться

210

Брюс Шнайер, «Why Cryptography Is Harder Than It Looks», *Information Security Bulletin*, 1997, Schneier on Security,

https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html.

Вернуться

211

«Keynote by Mr. Thomas Dullien – CyCon 2018», Центр НАТО по сотрудничеству в сфере кибероборонь, YouTube, 20 июня 2018 года, **https://www.youtube.com/watch?v=q98foLaAfX8**.

Вернуться

212

Пол Кохер, «Announce: Timing cryptanalysis of RSA, DH, DSS», sci.crypt, 11 декабря 1995 года, **https://groups.google.com/forum/#!msg/sci.crypt/OvUlewbjfa8/a1kP6WjW1lUJ**.

Вернуться

213

Пол Кохер, «Timing Attacks on Implementations of Diffie-H RSA, DSS, and Other Systems» в *материалах к 16-й ежегодной международной конференции по криптологии, посвященной прогрессу в криптологии*, конспекты лекций по компьютерным наукам 1109 (Springer, 1996), 104–13.

Вернуться

214

Оказывается, о некоторых угрозах, которые представляют атаки по сторонним каналам, разведывательным службам было известно намного раньше. Об этом свидетельствует статья 1972 года, рассекреченная в 2007: «TEMPEST: A Signal Problem», NSA *Cryptologic Spectrum* 2, № 3 (лето 1972): 26–30,

https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/tempest.pdf.

Вернуться

215

Эти сцены вполне могли бы быть позаимствованы из фильма о Джеймсе Бонде. В 2012 году испанский актер Хавьер Бардем сыграл злодея в фильме *007: Координаты «Скайфолл»* (режиссер Сэм Мендес, Columbia Pictures, 2012).

Вернуться

216

Это то же самое, что и с физическими ключами. Проще уследить за ключом от входной двери, чем обезопасить все имущество. Возможно, надежное хранение ключа является не настолько убедительной мерой безопасности, как наем команды охранников со злыми собаками, но это прагматичная альтернатива.

Вернуться

217

Использование паролей по умолчанию распространено намного шире, чем многие подозревают: «Risks of Default Passwords on the Internet», Агентство национальной безопасности США, 24 июня 2013 года, **https://www.us-cert.gov/ncas/alerts/TA13–175A**.

Вернуться

218

Веб-сайт, конечно, не предлагает открытый ключ лично *вам*; это происходит в фоновом режиме, и от вашего имени этот ключ получает ваш веб-браузер. Но, если вы зайдете в его настройки, у вас будет возможность взглянуть на эти ключи.

Вернуться

219

Вы можете отлично повеселиться и потерять уйму времени, исследуя разные мнения на эту тему. Одним из многих форумов, где обсуждается вопрос о существовании по-настоящему случайных значений, является Debate.org, где вы можете найти следующую дискуссию: «Philosophically and Rationally, Does Randomness or Chance Truly Exist?», Debate.org, **https://www.debate.org/opinions/philosophically-and-rationally-does-randomness-or-chance-truly-exist**.

Вернуться

220

Подбрасывание монеты может быть не настолько хорошим способом получения случайных значений, как многие считают. Исследование 2007 года показало, что монета, подброшенная вручную, имеет небольшую тенденцию приземляться в том положении, в котором она находилась изначально: Перси Диаконис, Сюзан Холмс и Ричард Монтгомери, «Dynamical Bias in the Coin Toss», SIAM Review 49, № 2 (April 2007): 211–35.

Вернуться

221

Интересным ресурсом на тему случайных значений является веб-сайт Random.org, **https://www.random.org** (по состоянию на 10 июня 2019 года). Там вы можете узнать больше о трудностях, связанных с генерацией по-настоящему случайных данных из физических источников, а также о том, как самостоятельно получить по-настоящему случайное число с помощью генератора на основе атмосферного шума.

Вернуться

222

Широкую огласку получила ситуация, возникшая в 2008 году, когда в операционной системе Debian для поддержки более старой версии протокола TLS использовался чрезвычайно плохой генератор псевдослучайных чисел. Он мог выдавать лишь небольшую часть «случайных» значений, необходимых для алгоритмов, которые он поддерживал: «Debian Security Advisory: DSA-1 1 openssl – Predictable Random Number Generator», Debian, 13 мая 2008 года, **https://www.debian.org/security/2008/dsa-1571**.

Вернуться

223

«Функция формирования ключа», Википедия, **https://ru.wikipedia.org/wiki/Функция_формирования_ключа** (по состоянию на 10 июня 2019 года).

Вернуться

224

Арьен К. Ленстра и др., «Ron Was Wrong, Whit Is Right», Cryptology ePrint Archive, 12 февраля 2012 года, **https://eprint.iacr.org/2012/064.pdf**.

Вернуться

225

Этот процесс регламентирован рядом стандартов безопасности для GSM, а также для 3G и 4G, в которых описываются средства криптографии, используемые в мобильных системах. Например, см. Джеффри Цихонски, Джошуа Франклин и Майкл Барток, «Guide to LTE Security», NIST Special Publication 800–187, 21 декабря 2017 года,

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800–187.pdf.

Вернуться

226

Если говорить о процедуре выбора общего закрытого ключа, вместо более классического гибридного шифрования предпочтение все чаще отдают протоколу согласования ключей Диффи-Хеллмана. Основная причина в том, что в случае раскрытия долгосрочного закрытого ключа это дает более высокую степень безопасности (это свойство иногда называют *совершенной прямой секретностью*). Подробности о протоколе Диффи-Хеллмана можно найти в практически любом учебнике по криптографии. Впервые он упоминается в статье Уитфилда Диффи и Мартина Хеллмана «New Directions in Cryptography», *IEEE Transactions on Information Theory* 22, № 6 (1976): 644–54.

Вернуться

227

Например, открытый ключ, основанный на 256-битных эллиптических кривых, зачастую представлен примерно 130 шестнадцатеричными символами.

Вернуться

228

Центром сертификации может быть любая организация, которой пользователи доверяют выпуск сертификатов. *Let's Encrypt* – это некоммерческий центр сертификации, созданный для поощрения широкого использования криптографии, в частности TLS, путем выпуска бесплатных сертификатов. Подробности можно найти на сайте Let's Encrypt, **https://letsencrypt.org** (по состоянию на 10 июня 2019 года).

Вернуться

229

Собака автора, упоминается в благодарностях.
Вернуться

230

Вышеупомянутые проблемы с плохо сгенерированными ключами RSA нельзя решить с помощью сертификации. Большинство из этих ключей были сертифицированы центрами, которые лишь подтверждали информацию о том, кто ими владеет, не ручаясь за их качество. Ситуация могла бы быть другой, если бы в обязанности центра сертификации входила генерация ключей. В данном случае центр мог заработать плохую репутацию из-за жалоб на недобросовестную практику и потерять доверие части пользователей.
Вернуться

231

Разработчики браузеров должны хранить списки корневых сертификатов, которые они согласились поддерживать в своем ПО. Например, список сертификатов, поддерживаемых компанией Apple, можно просмотреть на странице «Lists of Available Trusted Root Certificates in iOS», Apple, **https://support.apple.com/en-gb/HT204132** (по состоянию на 10 июня 2019 года).
Вернуться

232

Вы почти наверняка сталкивались с ситуацией, когда при попытке доступа к веб-странице вы получали предупреждение о сертификате, но игнорировали и скрывали его. Делая это, мы идем на риск. Такие предупреждения могут возникать из-за ошибок или неудачного

обновления сертификата, но причина также может быть и более серьезной, например, когда известно, что веб-сайт не заслуживает доверия.

Вернуться

233

Подробное исследование всех тонкостей управления сертификатами открытого ключа можно найти в книге Александра Вайсмайера *Introduction to Public Key Infrastructures* (Springer, 2013).

Вернуться

234

Нескончаемые, по-видимому, отчеты о масштабных утечках информации зачастую касаются баз данных, при сопровождении которых не соблюдаются меры предосторожности. *Общий регламент по защите данных* (англ. General Data Protection Regulation или GDPR) Европейского союза, вступивший в силу в мае 2018 года, отчасти посвящен предотвращению подобного рода происшествий.

Вернуться

235

Рекомендации об эффективном избавлении от данных можно найти, к примеру, в статье «Secure Sanitisation of Storage Media», Центр национальной компьютерной безопасности Великобритании, 23 сентября 2016 года, **https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media**.

Вернуться

236

Введение в аппаратные модули безопасности ищите в статье Джима Эттриджа «An Overview of Hardware Security Modules», SANS Institute

Information Security Reading Room, 14 января 2002 года, **https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757**.

Вернуться

237

Цитата позаимствована из колонки Джина Спаффорда «Rants & Raves», *Wired*, 25 ноября 2002 года.

Вернуться

238

Например, см. Арун Вишванат, «Cybersecurity's Weakest Link: Humans», *Conversation*, 5 мая 2016 года, **https://theconversation.com/cybersecuritys-weakest-link-humans-57455**.

Вернуться

239

Любая организация, которая защищает ноутбуки подобным образом, должна использовать аппаратные модули безопасности и серьезные административные процедуры для защиты главного ключа. Поэтому описанная здесь катастрофическая ситуация не должна произойти.

Вернуться

240

Первое в ряду научных исследований о трудностях, которые испытывают пользователи с программными средствами шифрования, принадлежит Альме Уиттон и Дж. Д. Тайгару, «Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0», из *материалов восьмого симпозиума USENIX по безопасности (Security '99)*, 23–26 августа 1999 года, Вашингтон, США (USENIX Association, 1999), 169–83.

Вслед за этим был научный труд Стива Шенга и др., «Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software», из *материалов второго симпозиума по практической конфиденциальности и безопасности* (ACM, 2006); и третьим в этом списке идет исследование Скотта Руоти и др., «Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client», arXiv, 13 января 2016 года, **https://arxiv.org/abs/1510.08555**. Вы можете видеть, к чему все идет, даже не читая эти материалы.

Вернуться

241

Стоит отметить, что эту проблему не всегда можно решить, отправляя пользователей на курсы повышения квалификации. Если система сложна в использовании, у нее по-прежнему будут постоянно возникать какие-то проблемы. И навыки, приобретенные во время обучения, можно быстро потерять, если не выполнять сложные задачи регулярно.

Вернуться

242

Аргумент о том, что плохая криптография иногда хуже, чем вообще никакой, приводит, к примеру, Эрез Метула в своей презентации «When Crypto Goes Wrong», OWASP Foundation, **https://appsec-labs.com/portal/wp-content/uploads/2011/09/When-Crypto-Goes-Wrong.pdf** (по состоянию на 10 июня 2019 года).

Вернуться

243

Одним из самых печально известных вирусов-вымогателей был WannaCry, который в мае 2017 года заразил свыше 200 000 компьютеров по всему миру. Средства защиты от него были разработаны относительно быстро, что позволило ограничить

нанесенный им ущерб. Если вы хотите познакомиться с этим видом вредоносного ПО и узнать, как с ним бороться, см. статью Джоша Фрулингера «What Is Ransomware? How These Attacks Work and How to Recover from Them», CSO, 19 декабря 2018 года, **https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html**.

Вернуться

244

Список реальных случаев, когда следователи по уголовным делам выступали против зашифрованных устройств, приводится в статье Клауса Шмеха «When Encryption Baffles the Police: A Collection of Cases», ScienceBlogs, **https://scienceblogs.de/klausis-krypto-kolumne/when-encryption-baffles-the-police-a-collection-of-cases/** (по состоянию на 10 июня 2019 года).

Вернуться

245

Есть некоторые основания полагать, что правоохранительные органы проводили кибератаки на сервисы, использовавшие Tor. Например, см. статью Девина Колдуэя «How Anonymous? Tor Users Compromised in Child Porn Takedown», NBC News, 5 августа 2013 года, **https://www.nbcnews.com/technolog/how-anonymous-tor-users-compromised-child-porn-takedown-6C10848680**.

Вернуться

246

Тот факт, что террористические группировки пользуются системами обмена сообщениями, спровоцировал некоторые из самых бурных споров вокруг шифрования: Гордон Рэйнер, «WhatsApp Accused of Giving Terrorists ‘a Secret Place to Hide’ as It Refuses to Hand Over London Attacker’s Messages», *Telegraph*, 27 марта 2017 года,

https://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide.

Вернуться

247

На самом деле шифрование с последующим выбрасыванием ключа иногда предлагается в качестве способа целенаправленного удаления данных на диске. Однако существуют некоторые веские аргументы в пользу того, что это не самый лучший подход: Сэмюель Пири, «Encryption Is NOT Data Sanitization – Avoid Risk Escalation by Mistaking Encryption for Data Sanitation», IAITAM, 16 октября 2014 года, **https://itak.iaitam.org/encryption-is-not-data-sanitization-avoid-risk-escalation-by-mistaking-encryption-for-data-sanitation**.

Вернуться

248

Доводы в пользу анализа входящего зашифрованного трафика приводятся, к примеру, в статье Пола Николсона «Let's Encrypt – but Let's Also Decrypt and Inspect SSL Traffic for Threats», Network World, 10 февраля 2016 года, **https://www.networkworld.com/article/3032153/let-s-encrypt-but-let-s-also-decrypt-and-inspect-ssl-traffic-for-threats.html**.

Вернуться

249

Именно это практически наверняка произошло в 2010 году, когда вирус Stuxnet заразил иранский завод по обогащению урана в Нетензе.

Вернуться

250

Фонд электронных рубежей дает рекомендации об инструментах, которые можно использовать для защиты конфиденциальности в Интернете. В большинстве своем они основаны на криптографии: «Surveillance Self-Defense», Фонд электронных рубежей, **https://ssd.eff.org** (по состоянию на 10 июня 2019 года).

Вернуться

251

Том Уайтхед, «Internet Is Becoming a ‘Dark and Ungoverned Space,’ Says Met Chief», Telegraph, 6 ноября 2014 года, **https://www.telegraph.co.uk/news/uknews/law-and-order/11214596/Internet-is-becoming-a-dark-and-ungoverned-space-says-Met-chief.html**.

Вернуться

252

«Director Discusses Encryption, Patriot Act Provisions», FBI News, 20 мая 2015 года, **https://www.fbi.gov/news/stories/director-discusses-encryption-patriot-act-provisions**.

Вернуться

253

«Cotton Statement on Apple’s Refusal to Obey a Judge’s Order to Assist the FBI in a Terrorism Investigation», Том Коттон, сенатор от штата Арканзас, 17 февраля 2016 года, **https://www.cotton.senate.gov/?p=press_release&id=319**.

Вернуться

254

«Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid», верховный комиссар ООН по правам человека, 4 марта

2016 года, **http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138**.

Вернуться

255

Эстер Дайсон, «Deluge of Opinions on the Information Highway», *Computerworld*, 28 февраля 1994 года, 35.

Вернуться

256

Дэвид Перера, «The Crypto Warrior», Politico, 9 декабря 2015 года, **https://www.politico.com/agenda/story/2015/12/crypto-war-cyber-security-encryption-000334**.

Вернуться

257

«Snowden at SXSW: ‘The Constitution Was Being Violated on a Massive Scale», RT, 10 марта 2014 года, **https://www.rt.com/usa/snowden-soghoian-sxsw-interactive-914**.

Вернуться

258

Эмбер Радд, «Encryption and Counter-terrorism: Getting the Balance Right», *Telegraph*, 31 июля 2017 года, **https://www.gov.uk/government/speeches/encryption-and-counter-terrorism-getting-the-balance-right**.

Вернуться

259

Оманд имел в виду принятие Акта о полномочиях следствия от 2016 года, который регламентирует разные аспекты перехвата данных. Цитата позаимствована из статьи Руби Лотт-Лавины «Can Governments Really Keep Us Safe from Terrorism without Invading Our Privacy?», *Wired*, 20 октября 2016 года, **https://www.wired.co.uk/article/david-omand-national-cyber-security**.

Вернуться

260

В 1996 году в *Вассенаарских соглашениях об экспортном контроле за традиционными вооружениями и товарами/технологиями двойного назначения* механизмы шифрования («криптография для конфиденциальности данных») были классифицированы как технология двойного назначения: «The Wassenaar Arrangement», **https://www.wassenaar.org** (по состоянию на 10 июня 2019 года).

Вернуться

261

Дилемма, связанная с применением шифрования, существовала еще до того, как криптографию начали использовать повсеместно, так как она является неотъемлемой частью его основной функции. Шифрование защищает секреты. С его помощью Мария Стюарт защищала свою частную жизнь и в то же время угрожала государственной власти. Что из этого было важнее, зависит от вашей точки зрения.

Вернуться

262

Называя эти методы *проблемными*, я вовсе не имею в виду, что их нужно избегать, а лишь указываю на то, что у них есть фундаментальные недостатки, которые сложно обойти.

Вернуться

263

Я специально высказываюсь здесь в провокационном ключе. Никто не просит сделать криптосистему небезопасной. Государству нужны альтернативные пути доступа к данным, защищенным с помощью криптографии. Но любые подобные средства, попавшие «не в те руки» (например, в руки преступников), будут считаться «взломом» криптосистемы.

Вернуться

264

Под *обычными пользователями* имеется в виду практически кто угодно, кроме самого государства. Это крайне упрощенный пример, как вы, я надеюсь, уже сами поняли.

Вернуться

265

Одной из первых компаний, которые начали предлагать такой криптографический продукт, была Crypto AG, основанная в Швейцарии в 1952 году и существующая по сей день: Crypto AG, **https://www.crypto.ch** (по состоянию на 11 августа 2019 года).

Вернуться

266

Уже давно ходят слухи, частично подкрепленные фактами о том, что в 1950-х компания Crypto AG сотрудничала с АНБ касательно продажи своих устройств некоторым странам: Готдон Корера, «How NSA and GCHQ Spied on the Cold War World», BBC, 28 июля 2015 года, **https://www.bbc.com/news/uk-33676028**.

Вернуться

267

Некоторые правительства почти наверняка занимаются разработкой собственных секретных алгоритмов для защиты своих данных, и в этом нет ничего плохого, если они обладают соответствующей квалификацией. Однако в наши дни правительство Руритании проявило бы неосмотрительность, слепо доверившись правительству Свободии с поставками технологий, в которых применяются секретные алгоритмы. В интересах Руритании было бы приобрести коммерческое оборудование с самыми передовыми публичными алгоритмами.

Вернуться

268

Например, см. статью Брюса Шнайера «Did NSA Put a Secret Backdoor in New Encryption Standard?», *Wired*, 15 ноября 2007 года, **https://www.wired.com/2007/11/securitymatters-1115**.

Вернуться

269

Отказ от Dual_EC_DRBG был анонсирован с статье «NIST Removes Cryptography Algorithm from Random Number Generator Recommendations», Национальный институт стандартов и технологий, 21 апреля 2014 года, **https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations**. Однако это произошло лишь через девять лет после того, как алгоритм Dual_EC_DRBG был одобрен в качестве стандарта для генерации псевдослучайных чисел. За это время он был внедрен в несколько широко известных средств безопасности, производители которых, предположительно, сотрудничали с АНБ: Джозеф Менн, «Exclusive: Secret Contract Tied NSA and Security Industry Pioneer», Reuters, 20 декабря 2013 года,

https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220.

Вернуться

270

Бывший глава АНБ Майкл Хайден высказывался о том, что некоторые из существующих криптосистем имеют уязвимости вида NOBUS (nobody-but-us – «никто, кроме нас»), которые, как он считает, могут эксплуатироваться только самим АНБ. Это очень неловкая идея; она подразумевает, что мы должны поверить не только в то, что АНБ использует уязвимости NOBUS этическим образом, но и в то, что эти уязвимости не могут быть обнаружены и использованы другими лицами: Андреа Питерсон, «Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws», *Washington Post*, 4 октября 2013 года, **https://www.washingtonpost.com/news/the-switch/wp/2013/10/04/why-everyone-is-left-less-secure-when-the-nsa-doesnt-help-fix-security-flaws**.

Вернуться

271

Например, см. «The Historical Background to Media Regulation», общедоступные учебные материалы Лестерского университета, **https://www.le.ac.uk/oerresources/media/ms7501/mod2unit11/page_02.htm** (по состоянию на 10 июня 2019 года).

Вернуться

272

Компания Global Partners Digital составила карту мира, на которой обозначены национальные ограничения и законы, касающиеся использования криптографии: «World Map of Encryption Laws and Policies», Global Partners Digital, **https://www.gp-digital.org/world-map-of-encryption** (по состоянию на 10 июня 2019 года).

Вернуться

273

Более широкое обсуждение политики вокруг криптографии во второй части двадцатого века, включая вопросы экспортных ограничений, можно найти в книге Стивена Леви *Crypto: Secrecy and Privacy in the New Cold War* (Penguin, 2002).

Вернуться

274

На знаменитые футболки с кодом RSA, которые считались военным снаряжением, можно посмотреть (и даже загрузить оригинальные иллюстрации, которые можно распечатать самостоятельно) на странице «Munitions T-Shirt», Cypherspace, **http://www.cypherspace.org/adam/uk-shirt.html** (по состоянию на 10 июня 2019 года).

Вернуться

275

Хороший обзор того, какое отношение к криптографии и ее способности изменить общество преобладало в то время, сделан в книге Томаса Рида *Rise of the Machines* (W. W. Norton, 2016). Еще один интересный взгляд на этот период предлагается в статье Арвинда Нараянана «What Happened to the Crypto Dream? Part 1», *IEEE Security & Privacy* 11, № 2 (март-апрель 2013 года): 75–76.

Вернуться

276

Томоти Мэй, «The Crypto Anarchist Manifesto», 22 ноября 1992 года, **https://www.activism.net/cypherpunk/crypto-anarchy.html**.

Вернуться

277

В 1991 году Фил Зиммерманн написал средство шифрования *Pretty Good Privacy* (*PGP*) и выложил его в свободный доступ. У проекта PGP было два спорных аспекта. Во-первых, шифрование, которое в нем использовалось, было достаточно устойчивым для того, чтобы подпадать под экспортные ограничения в США. Во-вторых, он применял алгоритм RSA, на который распространялись ограничения коммерческого лицензирования. Очень скоро PGP стал популярным во всем мире и получил широкое признание. Зиммерманн стал подозреваемым в уголовном деле о нарушении экспортного законодательства США, которое в итоге было закрыто.

Вернуться

278

В 1995 году криптограф Дэниел Бернштейн подал первый из целого ряда исков на правительство США, оспаривая экспортные ограничения в отношении криптографии. Аналогичное судебное разбирательство, *Юнгер против Дейли*, было начато в 1996 году.

Вернуться

279

С критикой идеи депонирования ключей с разных точек зрения можно ознакомиться во влиятельной научной работе Абельсона и др. «The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption», *World Wide Web Journal* 2, № 3 (1997): 241–57.

Вернуться

280

Этот девиз обычно ассоциируют с криптоанархистами 1990-х годов (он основан на другом похожем девизе, которое использует

американское оружейное лобби), и его можно встретить в документе, подготовленном для почтовой рассылки Cypherpunks: Тимоти Мэй, «The Cyphernomicon», 10 сентября 1994 года, **https://nakamotoinstitute.org/static/docs/cyphernomicon.txt**.

Вернуться

281

Акт о правовом регулировании следственных полномочий, часть III (Regulation of Investigatory Powers Act Part III или RIPA 3; принят в Великобритании в 2000 году) позволяет государству требовать раскрытия ключей шифрования или расшифровки. В соответствии с RIPA 3 некоторые люди в Великобритании были осуждены. Строго говоря, потеря ключа или невозможность его вспомнить не является оправданием, хотя можно представить ситуации, в которых это могло бы послужить состоятельным доводом в пользу защиты.

Вернуться

282

Просто попробуйте поискать эту фразу в Интернете. Вы будете поражены тем, сколько статей используют ее (или ее вариации) в качестве заголовка.

Вернуться

283

Некоторая информация из тысяч документов, разглашенных Сноуденом, была опубликована такими изданиями как *Guardian, Washington Post, New York Times, Le Monde* и *Der Spiegel*. Существует много ресурсов, посвященных этим разоблачениям. История об этой утечке освещена в книге Гленна Гринвальда *No Place to Hide* (Penguin, 2015), документальном фильме *Citizenfour. Правда Сноудена* (режиссер Лаура Пойтрас, HBO Films, 2014) и художественном фильме *Сноуден* (режиссер Оливер Стоун, Endgame Entertainment, 2016).

Вернуться

284

В Интернете есть несколько архивов, которые, по словам их создателей, содержат многие из этих документов, включая «Snowden Archive», Canadian Journalists for Free Expression, **https://www.cjfe.org/snowden** (по состоянию на 10 июня 2019 года).

Вернуться

285

В мае 2019 года было сообщено об уязвимости в системе обмена сообщениями WhatsApp, которая давала злоумышленникам доступ к данным смартфона. Обеспокоенность вызывало то, что для проведения атаки не требовалось участие со стороны пользователя; достаточно было позвонить на этот телефон: Лили Хэй Ньюман, «How Hackers Broke W App with Just a Phone Call», 14 мая 2019 года, **https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow**.

Вернуться

286

Эд Пилкингтон, «‘Edward Snowden Did This Country a Great Service. Let Him Come Home’», *Guardian*, 14 сентября 2016 года, **https://www.theguardian.com/us-news/2016/sep/14/edward-snowden-pardon-bernie-sanders-daniel-ellsberg**.

Вернуться

287

Проблема, вызванная сложностью киберпространства, усугубляется тем, что устройства становятся все более функциональными. Фил Зиммерманн высказал предположение о том, что «развитие технологий обычно ведет к упрощению слежения, а способность компьютеров отслеживать нас удваивается каждые восемь месяцев»: Ом Малик, «Zimmermann’s Law: PGP Inventor and Silent Circle Co-founder Phil Zimmermann on the Surveillance Society», GigaOm, 11 августа 2013 года, **https://gigaom.com/2013/08/11/zimmermanns-law-pgp-inventor-and-silent-circle-co-founder-phil-zimmermann-on-the-surveillance-society**.

Вернуться

288

Террористическая организация, деятельность которой запрещена на территории Российской Федерации.

Вернуться

289

Дэнни Ядрон, Спенсер Аккерман и Сэм Тилман, «Inside the FBI's Encryption Battle with Apple», *Guardian*, 18 февраля 2016 года, **https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple**.

Вернуться

290

Дэнни Ядрон, «Apple CEO Tim Cook: FBI Asked Us to Make Software 'Equivalent of Cancer'», *Guardian*, 25 февраля 2016 года, **https://www.theguardian.com/technology/2016/feb/24/apple-ceo-tim-cook-government-fbi-iphone-encryption**.

Вернуться

291

Рэйчел Робертс, «Prime Minister Claims Laws of Mathematics 'Do Not Apply' in Australia», *Independent*, 15 июля 2017 года, **https://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-mathematics-do-not-apply-australia-encryption-l-a7842946.html**.

Вернуться

292

Информацию о размере сети Tor можно найти на странице «Tor Metrics», Tor Project, **https://metrics.torproject.org/networksize.html** (по состоянию на 10 июня 2019 года).

Вернуться

293

Например, см. Ханна Кюхлер, «Tech Companies Step Up Encryption in Wake of Snowden», *Financial Times*, 4 ноября 2014 года, **https://www.ft.com/content/3c1553a6–6429-11e4-bac8–00144feabdc0**.

Вернуться

294

«National Cyber Security Strategy 2016–2021», правительство Великобритании, 2016, **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf**. Национальная стратегия кибербезопасности Великобритании четко определяет важную роль широкого применения шифрования, отмечая, что «криптографические средства имеют основополагающее значение для защиты нашей наиболее конфиденциальной информации и выбора того, как использовать вооруженные силы и службы национальной безопасности».

Вернуться

295

В 2015 году группа ведущих криптографов обозначила угрозы безопасности, возникающих из-за целого ряда методов организации доступа правоохранительных органов к зашифрованным средствам связи. См. Хал Абелсон и др., «Keys under Doormats», *Communications of the ACM* 58, № 10 (2015): 24–26.

Вернуться

296

«Remarks by the President at South by Southwest Interactive», Белый дом, офис пресс-секретаря, 11 марта 2016 года, **https://obamawhitehouse.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive**.

Вернуться

297

Не все способы законного доступа к данным являются одинаково приемлемыми для общества, поэтому для определения наиболее подходящего компромисса лучше всего использовать комплексный подход: Эндрю Кин Вудс, «Encryption Substitutes», Гуверовский институт, Aegis Paper Series № 1705, 18 июля 2017 года, **https://www.scribd.com/document/354096059/Encryption-Substitutes#from_embed**.

Вернуться

298

Я говорю *традиционно*, поскольку мобильные и стационарные телефонные сети все теснее интегрируются, а шифрование, которое когда-то защищало только первый отрезок между мобильным телефоном и базовой станцией, проникает в эти сети глубже, чем раньше.

Вернуться

299

Суть в следующем: если мы собираемся заново спроектировать архитектуру Интернета и заново согласовать безопасность в ее рамках, необходимо подумать о том, какой уровень безопасности требуется для тех или иных сервисов. Очевидно, что современное сквозное

шифрование является предметом серьезной обеспокоенности для правоохранительных органов. Чтобы как следует согласовать дальнейший план действий, все стороны, участвующие в этом процессе, должны быть готовы на компромисс. Единственной вероятной альтернативой является продолжение конфликта.

Вернуться

300

«Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms (SALT II)», Бюро по вопросам контроля за вооружениями, проверки и соблюдения, 1979 год, **https://2009–2017.state.gov/t/isn/5195.htm**.

Вернуться

301

Дэниел Мур и Томас Рид, «Cryptopolitik and the Darknet», *Survival* 58, № 1 (2016): 7–38.

Вернуться

302

Строго говоря, аналогия должна выглядеть так: вы кладете копию письма в каждый из новых сейфов и отдаете эти сейфы своим врагам; в результате у каждого врага теперь есть одна копия письма в сейфе с возможностью взлома и другая в сейфе, который нельзя взломать.

Вернуться

303

Этот аргумент особенно актуален для шифрования. Для других криптографических средств, таких как целостность данных, ситуация может быть не настолько серьезной. Например, если алгоритм цифровой подписи взломан и требует обновления, мы можем заново

подписать данные с помощью нового алгоритма. Проблемы возникнут лишь в случае, если старый алгоритм, который использовался в момент первоначального создания подписей, был недостаточно устойчивым.

Вернуться

304

Поскольку криптографические алгоритмы зачастую требуют много вычислительных ресурсов, во многих сферах применения криптографии они реализованы на аппаратном, а не на программном уровне. Например, когда в 2003 году из-за обнаружения ряда криптографических уязвимостей протокол безопасности Wi-Fi WEP был объявлен устаревшим, не все устройства можно было перевести на новые протоколы. В связи с этим перед некоторыми пользователями беспроводных сетей стоял следующий выбор: купить новое устройство или дальше использовать небезопасную криптографию.

Вернуться

305

Квантовую механику принято считать таинственной, парадоксальной и недоступной для понимания большинству из нас, и не последнюю роль в этом играет экспертное сообщество. Многие приписывают лауреату Нобелевской премии, физику Нильсу Бору следующее высказывание: «Если вас не шокирует квантовая теория, вы ее не понимаете». Даже популярные объяснения квантовых концепций обычно преподносятся, как нечто непознаваемое; в качестве примеров можно привести книги Джима Аль-Халили *Quantum: A Guide for the Perplexed* (Weidenfeld & Nicolson, 2012) и Маркуса Чауна *Quantum Theory Cannot Hurt You* (Faber & Faber, 2014).

Вернуться

306

Квантовая генерация случайных чисел доступна для коммерческого использования с начала этого века и основана на разных видах квантовых измерений. Например, см. «What Is the Q in QRNG?», ID Quantique, октябрь 2017 года, **https://www.idquantique.com/random-number-generation/overview**, и «NIST's New Quantum Method Generates Really Random Numbers», Национальный институт стандартов и технологий, 11 апреля 2018 года, **https://www.nist.gov/news-events/news/2018/04/nists-new-quantum-method-generates-really-random-numbers**.

Вернуться

307

Относительно доступным экскурсом в историю разработки квантовых компьютеров является книга Джона Гриббина *Computing with Quantum Cats: From Colossus to Qubits* (Black Swan, 2015).

Вернуться

308

В случае, если вы никогда не швыряли злыми птичками по свиньям (что вряд ли), это отсылка к феноменально успешной серии игр *Angry Birds* от Rovio Entertainment Corporation.

Вернуться

309

Существуют разные взгляды на то, как будут развиваться квантовые вычисления в будущем, равно как и на потенциальные последствия. Но, похоже, все согласны с тем, что мощные квантовые компьютеры станут реальностью… когда-нибудь!

Вернуться

310

Алгоритм, опубликованный в 1994 году математиком Питером Шором и впоследствии названный в его честь, продемонстрировал, что квантовый компьютер способен как разлагать на множители, так и вычислять дискретные логарифмы. Оригинальная статья: Питер Шор, «Algorithms for Quantum Computation: Discrete Logarithms and Factoring», *из материалов 35-го ежегодного симпозиума по основам компьютерных наук* (IEEE Computer Society Press, 1994), 124–34. Позже алгоритм Шора начали использовать для поиска множителей у относительно небольших чисел на только появившихся квантовых компьютерах.

Вернуться

311

В 2016 году Национальный институт стандартов и технологий США запустил программу по разработке и анализу постквантовых алгоритмов асимметричного шифрования, которые должны быть устойчивы к квантовым вычислениям. Как ожидается, этот процесс займет по меньшей мере шесть лет: «Post-q Cryptography Standardization», NIST Computer Security Resource Center, **https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization** (обновлено 10 июня 2019 года).

Вернуться

312

В 1996 году специалист в области компьютерных наук Лов Гровер предложил алгоритм (впоследствии названный в его честь), который показывает, что квантовые вычисления могут уменьшить время, необходимое для поиска ключей методом полного перебора, до корня изначального показателя. Это означает, что на квантовом компьютере полный перебор, скажем, 2^{128} ключей займет «лишь» время, которое нужно для перебора 2^{64} ключей. Следовательно, чтобы сохранить нынешний уровень безопасности с учетом квантовых вычислений, длина симметричных ключей должна удвоиться. Однако стоит

отметить, что этот алгоритм нуждается в огромном объеме квантовой памяти. Оригинальная статья: Лов К. Гровер, «A Fast Quantum Mechanical Algorithm for Database Search», *из материалов двадцать восьмого ежегодного симпозиума ACM по теории вычислений* (ACM, 1996), 212–19.

Вернуться

313

Доступное объяснение квантового распространения ключей можно найти в книге Саймона Сингха *The Code Book* (Fourth Estate, 1999).

Вернуться

314

Краткий обзор некоторых реальных трудностей, возникающих при использовании квантового распространения ключей, можно найти в статье Элени Диаманти и др., «Practical Challenges in Quantum Key Distribution», *npj Quantum Information 2*, статья № 16025 (2016).

Вернуться

315

Шифр одноразовых блокнотов является чрезвычайно простым алгоритмом шифрования, современную версию которого иногда называют *шифром Вернама*. Он подразумевает шифрование каждого исходного бита путем добавления ключевого бита, сгенерированного случайным образом. В 1949 году Клод Шеннон показал, что шифр одноразовых блокнотов является единственным «идеальным» алгоритмом шифрования в том смысле, что злоумышленник не может узнать из шифротекста ничего (нового) об исходных данных. К сожалению, одно из его строгих требований заключается в использовании по-настоящему случайных ключей той же длины, что и исходные данные, и эти ключи должны генерироваться отдельно для

каждого бита, что делает этот шифр непрактичным в большинстве ситуаций.

Вернуться

316

Разновидности всех этих предметов с поддержкой интернет-соединения были доступны в качестве коммерческих продуктов в 2017 году: Мэтт Рейнольдс, «Six Internet of Things Devices That Really Shouldn’t Exist», *Wired*, 12 мая 2017 года, **https://www.wired.co.uk/article/strangest-internet-of-things-devices**.

Вернуться

317

Сложно точно предсказать, насколько распространенным будет Интернет вещей в будущем, но такие организации как Gartner и GSMA Intelligence неизменно утверждают, что к 2025 году общемировое число подключенных к Интернету IoT-устройств достигнет порядка 25 миллиардов. Какими бы ни были точные цифры, недостатка в этих устройствах точно не будет!

Вернуться

318

Многие устройства, подключенные к Интернету, имеют плохую защиту (или вообще никакой). В будущем перед нами стоит серьезный вызов: убедить поставщиков, сети розничной продажи и регулирующие органы в том, что технологии IoT необходимо сделать достаточно защищенными. Например, см. «Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report», Департамент цифровых технологий, культуры, СМИ и спорта, правительство Великобритании, март 2018 года, **https://www.gov.uk/government/publications/secure-by-design**.

Вернуться

319

В августе 2018 года Национальный институт стандартов и технологий организовал конкурс в стиле AES по разработке новых криптографических алгоритмов, которые можно было бы использовать в ограниченных окружениях, где традиционные алгоритмы вроде AES не подходят: «Lightweight Cryptography», NIST Computer Security Resource Center, **https://csrc.nist.gov/Projects/Lightweight-Cryptography** (обновлено 11 июня 2019 года).

Вернуться

320

Дэвид Талбот, «Encrypted Heartbeats Keep Hackers from Medical Implants», MIT *Technology Review*, 16 сентября 2013 года, **https://www.technologyreview.com/2013/09/16/176454/encrypted-heartbeats-keep-hackers-from-medical-implants**.

Вернуться

321

Самые очевидные угрозы заключаются в раскрытии, повреждении и потере данных. Однако самым вероятным последствием является то, что из этих данных попытаются извлечь прибыль. Действительно, пользовательские данные могут находиться в основе коммерческого предложения многих (бесплатных) облачных сервисов.

Вернуться

322

Краткий обзор и дополнительные ссылки на средства криптографии, предназначенные для облачных хранилищ, можно найти в разделе «Cryptographic Tools for Cloud Environments» книги Джеймса Алдермана, Джейсона Крэмптона и Кейт М. Мартин *Guide to Security*

Assurance for Cloud Computing, редакторы Шао Ин Чу, Ричард Хилл и Марселло Тровати (Springer, 2016), 15–30.

Вернуться

323

Первый *полностью гомоморфный* метод шифрования предложил Крейг Джентри в своей докторской диссертации «A Fully Homomorphic Encryption Scheme» (Стэнфордский университет, 2009 год), **https://crypto.stanford.edu/craig/craig-thesis.pdf**. К сожалению, этот метод совершенно непрактичный ввиду низкой скорости работы и высоких требований к вычислительным ресурсам. В 2017 году Дэвид Арчер из научно-исследовательской фирмы Galois, в которой он работал над тем, чтобы сделать этот алгоритм «приходным к практическому применению», признал, что, несмотря на повышение скорости, «мы все еще далеки от обработки в реальном времени»: Боб Браун, «How to Make Fully Homomorphic Encryption 'Practical and Usable», *Network World*, 15 мая 2017 года, **https://www.networkworld.com/article/3196121/how-to-make-fully-homomorphic-encryption-practical-and-usable.html**.

Вернуться

324

Питер Рейчек, «Can Futurists Predict the Year of the Singularity?», Singularity Hub, 31 мая 2017 года, **https://singularityhub.com/2017/03/31/can-futurists-predict-the-year-of-the-singularity/#sm.00001v8dyh0rpmee8xcj52fjo9w33**.

Вернуться

325

Хорошее введение в искусственный интеллект и то, как его развитие может изменить наше обществе, можно найти в книгах Макса

Тегмарка *Life 3.0: Being Human in the Age of Artificial Intelligence* (Penguin, 2018) и Ханны Фрай *Hello World* (Doubleday, 2018).
Вернуться

326

Эти цифры взяты из презентации «Data Never Sleeps 6.0», Domo, **https://www.domo.com/learn/data-never-sleeps-6** (по состоянию на 10 июня 2019 года).
Вернуться

327

Сбор данных и их обработку в крупных масштабах иногда называют *большими данными* (от англ. big data). Познакомиться с возможными последствиями использования больших данных можно в книгах *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2013) Виктора Майера-Шенбергера и Кеннета Кукьера, а также *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton, 2015) Брюса Шнайера.
Вернуться

328

Майлз Брандейдж и др. подготовили интересный отчет о потенциальных последствиях развития искусственного интеллекта для кибербезопасности: «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation», февраль 2018 года, **https://maliciousaireport.com**.
Вернуться

329

Мои наблюдения относительно тесной связи между криптографией и доверием вдохновлены выступлением профессора Ликун Чен на

Первом криптодне Лондона в Королевском колледже при Лондонском университете, 5 июня 2017 года.
Вернуться

330

Lexico, «Trust», **https://www.lexico.com/en/definition/trust** (по состоянию на 12 июня 2019 года).
Вернуться

331

Документы, раскрытые Сноуденом, касались методов, которыми правительства пытались получить контроль за криптографией, однако это подорвало доверие некоторых людей к криптографии как таковой, что, наверное, было неизбежно.
Вернуться

332

Отличную книгу о формировании широкого доверия в обществе с перспективой повторения этого опыта в киберпространстве написал Брюс Шнайер: *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (Wiley, 2012).
Вернуться

333

Подробности о состоявшихся и будущих симпозиумах Real World Crypto можно найти на веб-сайте «Real World Crypto Symposium», Международная ассоциация криптологических исследований (по состоянию на 12 июня 2019 года).
Вернуться