КИТ МАРТИН

КРИПТОГРАФИЯ

КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ

АЛГОРИТМЫ ШИФРОВАНИЯ | МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ | ПРОТОКОЛЫ БЕЗОПАСНОСТИ

БОМБОРА
ИЗДАТЕЛЬСТВО

Кит Мартин

Криптография. Как защитить свои данные в цифровом пространстве

Серия «БукТех. Книги про технологии»

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=68717130
К. Мартин. Криптография. Как защитить свои данные в цифровом пространстве: ООО «Издательство «Эксмо»; Москва; 2023
ISBN 978-5-04-178707-3

Аннотация

Криптография – ключ к цифровой безопасности. Имея базовое представление о ней, вы сможете не только защитить свои данные от угроз, кроющихся в киберпространстве, но и лучше понять природу интернет-технологий, все глубже внедряющихся в нашу повседневную жизнь. Каковы потенциальные последствия подключения к незащищенной сети Wi-Fi? Так ли уж важно иметь разные пароли для разных учетных записей? Если вы видите, что у веб-сайта нет действительного сертификата, стоит ли продолжать с ним работу? Ответы на эти и другие вопросы вы найдете внутри.

В формате PDF A4 сохранен издательский макет книги.

Содержание

Кит Мартин
Криптография. Как защитить свои данные в цифровом пространстве

Keith Martin
Cryprography: The Key to Digital Security, How It Works, and Why It Matters

* * *

Посвящается Фреду: криптографу, визионеру, наставнику

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

[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**.

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?

---

[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**.

[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**.

[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**.

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].

---

[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.

[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!

[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.

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]».

---

[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.

[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 аб-

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 выделен-

---

стрaктном 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*».

ными 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 ез-

[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.

дить 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 прихо-

---

[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**.

[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

дился 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, до-

---

Fraud Survey 2018», PwC, 2018, **https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html**.

[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**.

[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).

ходы 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 пользуе-

---

[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**.

тесь 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

[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://**

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 ки-

---

www.krackattacks.com.

[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**.

[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**.

бербезопасностью 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

[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**.

[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**.

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 внутрен-

---

[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.

[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**.

[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**.

них 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?

---

[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**.

[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**.

[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 сво-

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, ка-

---

их 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**.

[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**.

[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**.

кую 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 сосредото-

[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*

чимся 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 опреде-

---

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.

[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.

[31] Если этот шифр вам не поддался, попробуйте сдвинуть буквы вперед на одну позицию в алфавите! – *Здесь и далее прим. ред.*

ление 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 материаль-

ных 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 са-

мом 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 ха-

рактерный 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 надпи-

си, 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 –

[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).

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 мно-

---

[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**.

гих 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 уго-

---

[34] Это не совсем точно, поскольку людям свойственно переоценивать одни угрозы, такие как авиакатастрофы, и существенно недооценивать другие, например, загрязнение воздуха.

[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**.

[36] Для нашего читателя этот раздел может быть довольно забавен, поскольку именно такие аферы с платежками в последние несколько лет происходят постоянно и массово.

няют 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

[37] Стефани Хоэл и др., «Itsy Bitsy Spider. .: Infants React with Increased Arousal to Spiders and Snakes», *Frontiers in Psychology* 8 (2017): 1710.

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.

---

[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**.

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 ка-

кой-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 успеш-

---

[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.

ных 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 про-

[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).

мыслов 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

[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.

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,*

[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**.

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

---

[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**.

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].

---

[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**.

[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.

[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, поделив-

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

шись 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.

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, кибер-

защиты 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].

[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 кана-

лов 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).

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 *толь-*

ко 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 обеспе-

---

[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».

[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.

чиваться 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, ком-

пьютер 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 при-

мере 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.

---

[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.

[51] Длину ключа иногда называют *размером*. Я буду считать эти термины синонимами.

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

---

[52] Количество абонентов мобильной связи в мире насчитывает более 5 миллиардов: «The Mobile Economy 2019», Ассоциация GSM, 2019 год, **https://www.gsma.com/mobileeconomy**.

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 забо-

---

[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!

тит, 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 без-

---

[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.

опасности 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 неза-

[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.

щищенным 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.

---

[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).

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.

Конец ознакомительного фрагмента.