Содержание

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 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*).

В главе 2 я покажу, что такое безопасность в киберпространстве, и как криптография помогает ее обеспечить.

---

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