Введение

Существуют два вида криптографии: криптография, которая помешает вашей младшей сестре читать ваши файлы, и криптография, которая помешает читать ваши файлы правительствам ведущих стран мира. Эта книга о криптографии второго типа.

Если я спрячу письмо в сейфе где-нибудь в Нью-Йорке, а затем попрошу вас прочитать его, то это не безопасность, а ее имитация. С другой стороны, если я запру письмо в сейфе и передам вам этот сейф вместе с инструкцией и сотней аналогичных сейфов со всеми их комбинациями, чтобы вы и лучшие в мире специалисты по взлому могли изучить запирающий механизм, а вы все равно не сможете открыть этот сейф и прочитать письмо — вот что такое безопасность.

Долгие годы криптография этого вида использовалась исключительно в военных целях. Агентство национальной безопасности Соединенных Штатов Америки (АНБ США) и аналогичные ведомства в бывшем Советском Союзе, Англии, Франции, Израиле и других странах потратили миллиарды долларов, пытаясь обеспечить безопасность собственных линий связи, в то же время пытаясь взломать все остальные. Частные лица, имеющие значительно меньше опыта и денег, были бессильны защитить свою конфиденциальную информацию от правительств.

За последние двадцать лет количество открытых научных исследований в области криптографии резко выросло. Со времен Второй мировой войны компьютерная криптография во всем мире применялась исключительно в военной области, а рядовые граждане пользовались классической криптографией. В настоящее время компьютерная криптография вышла за пределы военной области. Теперь дилетанты получили средства долгосрочной защиты от самых могущественных противников, в том числе от военных ведомств.

Нужна ли среднестатистическим людям такая степень безопасности? Да. Они могут планировать политические кампании, обсуждать схемы уклонения от налогов и заниматься противоправной деятельностью. Они могут проектировать новую продукцию, обсуждать стратегию маркетинга или планировать недружественное поглощение конкурентов. Они могут жить в стране, которая не уважает неприкосновенности частной жизни своих граждан. Они могут делать нечто, по их мнению, вполне законное, хотя это не так. Как бы то ни было, данные и линии связи должны быть персональными, конфиденциальными и недоступными для посторонних.

Эта книга выходит в свет в очень неспокойное время. В 1994 году администрация Клинтона (Clinton) приняла стандарт шифрования с депонированием ключей (Escrowed Encryption Standard), включая микросхему Clipper и плату Fortezza, и подписала закон о цифровой телефонии. Эти инициативы направлены на расширение возможностей правительства в области электронной слежки.

Сбываются некоторые из мрачных предсказаний Оруэлла: правительство имеет право подслушивать личные разговоры, а с человеком, пытающимся скрыть свои секреты от правительства, могут произойти неприятности. Законодательство всегда разрешало слежку по решению суда, но впервые люди сами должны предпринимать активные действия, чтобы облегчить слежку за ними. Эти инициативы — не просто предложения правительства в какой-то малозначимой сфере; это превентивные и односторонние попытки узурпировать права, ранее принадлежавшие народу.

Законы о микросхеме Clipper и цифровой телефонии не защищают конфиденциальность. С их помощью правительство хочет заставить людей поверить, будто оно уважает их тайны. Те же силовые структуры, которые незаконно записывали телефонные разговоры Мартина Лютера Кинга (Martin Luther King Jr.), могут легко прослушивать телефон, защищенный микросхемой Clipper. В недавнем прошлом местные полицейские власти были привлечены к криминальной или гражданской ответственности за незаконное прослушивание во многих штатах — в Мэриленде, Коннектикуте, Вермонте, Джорджии, Миссури и Неваде. Идея реализовать технологию, которая способствует появлению полицейского государства, — плохая идея.

Следовательно, недостаточно защитить себя законами, необходимо защитить себя математикой. Шифрование — слишком важное дело, чтобы доверять ее правительствам.

Эта книга даст вам инструменты для защиты ваших секретов; криптографические программы можно объявить вне закона, но саму информацию — никогда.

Как читать эту книгу

Я писал *Прикладную криптографию* и как неформальное введение, и как полный справочник. Я старался писать понятно, в то же время не жертвуя точностью. Тем не менее эту книгу не следует считать математической монографией. Хотя я не прибегал к умышленному искажению информации, но, чтобы сохранить темп изложения, я не приводил теоретические сведения. Для читателей, интересующихся формальной теорией, в конце книги приведены многочисленные ссылки на научную литературу.

Глава 1 представляет собой введение в криптографию. В ней приводятся определения многих терминов и кратко описывается криптография, использовавшаяся до появления компьютеров.

В главах 2–6, образующих часть I, описываются криптографические протоколы: что люди могут делать с помощью криптографии. Протоколы бывают простыми (передача шифрованных сообщений от одного человека другому), сложными (жеребьевка с помощью монеты по телефону) и эзотерическими (безопасное и анонимное обращение электронных денег). Некоторые из этих протоколов являются очевидными, другие — просто потрясающими. Криптография может решить множество проблем, о которых большинство людей даже не подозревает.

В главах 7–10, составляющих часть II, обсуждаются криптографические методы. Все эти четыре главы имеют большое значение для самых распространенных применений криптографии. Главы 7 и 8 посвящены ключам: какой должна быть длина безопасного ключа, как генерировать, хранить и распределять ключи и т.д. Управление ключами представляет собой самую трудную часть криптографических механизмов и часто является уязвимым местом систем, которые во всем остальном совершенно безопасны. В главе 9 обсуждаются разные способы использования криптографических алгоритмов, а глава 10 содержит вспомогательную информацию об алгоритмах — как их выбирать, реализовывать и применять.

Каждая из глав 11–23, образующих часть III, посвящена отдельному криптографическому алгоритму. Глава 11 содержит основные математические сведения. Ее обязательно следует прочитать, если только вы интересуетесь алгоритмами с открытыми ключами. Если же вы собираетесь использовать алгоритм DES (или что-нибудь аналогичное), то ее можно пропустить. В главе 12 обсуждается алгоритм DES: его сущность, история, безопасность и варианты. Главы 13–15 посвящены другим блочным алгоритмам. Если вам нужно что-то более безопасное, чем алгоритм DES, то переходите к разделам, в которых описываются алгоритмы IDEA и тройной DES. Если вас интересуют другие алгоритмы, некоторые из которых могут быть безопаснее DES, прочитайте всю главу. В главах 16 и 17 рассматриваются потоковые алгоритмы. В центре внимания главы 18 находятся однонаправленные хешфункции, среди которых самыми распространенными являются функции MD5 и SHA, хотя наряду с ними рассматриваются и многие другие. Глава 19 посвящена алгоритмам шифрования с открытым ключом; глава 20 — алгоритмам цифровой подписи с открытым ключом; глава 21 — алгоритмам идентификации с открытым ключом; глава 22 — алгоритмам обмена ключами в криптогра-

фических системах с открытым ключом. Самыми важными являются алгоритмы RSA, DSA, Фиата-Шамира (Fiat–Shamir) и Диффи-Хелмана (Diffie–Hellman). В главе 23 описываются эзотерические алгоритмы и протоколы с открытым ключом; в этой главе используется достаточно сложная математика, так что приготовьтесь к испытаниям.

Главы 24 и 25, составляющие часть IV, посвящены реальному миру криптографии. В главе 24 обсуждаются некоторые современные реализации алгоритмов и протоколов, а глава 25 касается некоторых политических вопросов, связанных с криптографией. Несомненно, эти главы не являются исчерпывающими.

Кроме того, в части III обсуждаются исходные коды 10 алгоритмов. Весь код, который я хотел включить в книгу, привести невозможно из-за его огромного объема. К тому же криптографические исходные коды в любом случае нельзя экспортировать. (Забавно, что Госдепартамент разрешил экспортировать первое издание этой книги с исходным кодом, но не разрешил экспортировать компьютерный диск с теми же самыми исходными кодами. Попробуй пойми.) Набор дисков с исходным кодом, прилагаемый к этой книге, содержит намного больше исходных кодов, чем я смог включить в книгу, возможно, это крупнейшая коллекция криптографических исходных кодов, существующая за пределами военных ведомств. В данный момент я могу прислать эти диски с исходным кодом только гражданам США и Канады, живущим в этих странах, но, возможно, когда-нибудь ситуация изменится. Если вы собираетесь использовать или испытывать криптографические алгоритмы, описанные в книге, постарайтесь добыть этот диск.

Одним из недостатков книги является то, что из-за энциклопедического характера ее иногда трудно понять. Это правда, но я хотел написать единый справочник для тех, кто мог встретиться с каким-либо алгоритмом в научной литературе или в ходе работы. Заранее приношу свои извинения тем читателям, которым нужен учебник по криптографии. Впервые многое из того, чтобы было сделано в области криптографии, изложено в одной книге. И все же из-за ограничения объема я был вынужден отказаться от изложения многих вопросов. Я включил в книгу темы, которые показались мне важными, практичными или интересными. Если я не мог дать глубокое изложение темы, то приводил ссылки на соответствующие работы.

Я приложил максимум усилий, пытаясь обнаружить и устранить все ошибки в книге, но многие люди уверяли меня, что это просто невозможно. Конечно, во втором издании содержится намного меньше опечаток, чем в

первом. Перечень ошибок можно получить у меня.[1] Кроме того, он периодически рассылается в телеконференции Usenet `sci.crypt`. Если вы обнаружите ошибку, пожалуйста, сообщите мне об этом. Каждому, кто первым обнаружит данную ошибку в книге, я бесплатно пришлю диск с исходным кодом[2].

Благодарности

Перечень людей, причастных к созданию этой книги, может показаться бесконечным, но все они достойны упоминания. Мне хотелось бы поблагодарить Дона Альвареса (Don Alvarez), Росса Андерсона (Ross Anderson), Дэйва Бейленсона (Dave Balenson), Карла Бармса (Karl Barms), Стива Белловина (Steve Bellovin), Дэна Бернстайна (Dan Bernstein), Эли Байем (Ell Biham), Джоан Бояр (Joan Boyar), Карен Купер (Karen Cooper), Вита Диффи (Whit Diffie), Джоан Фейгенбаум (Joan Feigenbaum), Фила Карна (Phil Karn), Нила Коблица (Neal Koblitz), Ксуейа Лай (Xuejia Lai), Тома Леранта (Tom Leranth), Майка Марковица (Mike Markowitz), Ральфа Меркла (Ralph Merkle), Билла Паттена (Bill Patten), Питера Пирсона (Peter Pearson), Чарльза Пфлегера (Charles Pfleeger), Кена Пиццини (Ken Pizzini), Барта Пренела (Bart Preneel), Марка Риордана (Mark Riordan), Йоахима Шурмана (Joachim Schurman) и Марка Шварца (Marc Schwartz) за чтение и редактирование всего первого издания или его частей; Марка Воклера (Marc Vauclair) за перевод первого издания на французский; Эйба Абрахама (Abe Abraham), Росса Андерсона (Ross Anderson), Дэйва Бенисара (Dave Banisar), Стива Белловина (Steve Bellovin), Эли Байем (Ell Biham), Мэтта Бишопа (Matt Bishop), Мэтта Блэйза (Matt Blaze), Гэри Картера (Gary Carter), Жана Комениша (Jan Comenisch), Клода Крепо (Claude Crepeau), Йона Дамана (Joan Daemon), Хорхе Давила (Jorge Davila), Эда Доусона (Ed Dawson), Вита Диффи (Whit Diffie), Карла Эллисона (Carl Ellison), Джоан Фейгенбаум (Joan Feigenbaum), Нильса Фергюсона (Niels Ferguson), Матта Франклина (Matt Franklin), Розарио Сеннаро (Rosario Cennaro), Дитера Колмана (Dieter Collmann), Марка Горески (Mark Goresky), Ричарда Грэйвмана (Richard Graveman), Стюарта Хабера (Stuart Haber), Джингмана Хе (Jingman He), Боба Хэйга (Bob Hague), Кеннета Айверсона (Kenneth Iversen), Маркуса Джекобсона (Markus Jakobsson), Берта Калиски (Burt Kaliski), Фила Кана (Phil Karn), Джона Келси (John Kelsey), Джона

[1] Ошибки, замеченные автором во всех выпусках второго издания, а также его комментарии и уточнения к устаревшей информации см. в разделе `Second Edition Errata` на сайте `https://www.schneier.com/books/applied_cryptography/errata.html`. — *Примеч. ред.*

[2] Это относится только к гражданам США и Канады. — *Примеч. ред.*

Кеннеди (John Kennedy), Ларса Кнудсена (Lars Knudsen), Пола Кочера (Paul Kocher), Джона Лэдвига (John Ladwig), Ксуейа Лай (Xuejia Lai), Аджена Ленстры (Arjen Lenstra), Пола Лейланда (Paul Leyland), Майка Марковица (Mike Markowitz), Джима Мэсси (Jim Massey), Брюса МакНейра (Bruce McNair), Вильяма Хью Мюррея (William Hugh Murray), Роджера Нидхэма (Roger Needham), Клифа Неймана (Clif Neuman), Кейсу Найберг (Kaisa Nyberg), Люка О'Коннора (Luke O'Connor), Питера Пирсона (Peter Pearson), Рене Перальта (Rene Peralta), Барта Пренела (Bart Preneel), Израиля Радай (Yisrael Radai), Мэтта Робшоу (Matt Robshaw), Майкла Роу (Michael Roe), Фила Рогуэя (Phil Rogaway), Эви Рубина (Avi Rubin), Пола Рубина (Paul Rubin), Селвина Рассела (Selwyn Russell), Казуе Сако (Kazue Sako), Махмуда Салмасизадеха (Mahmoud Salmasizadeh), Маркуса Стадлера (Markus Stadler), Дмитрия Титова (Dmitry Titov), Джимми Аптона (Jimmy Upton), Марка Воклера (Marc Vauclair), Сержа Воденея (Serge Vaudenay), Гидеона Ювала (Gideon Yuval), Глена Зорна (Glen Zorn) и многих безымянных правительственных служащих за чтение и редактирование всего второго издания или его частей; Лори Брауна (Lawrie Brown), Лизу Кэндл (Leisa Candle), Джоан Дэймон (Joan Daemon), Питера Гутмана (Peter Gutmann), Алана Инсли (Alan Insley), Криса Джонстона (Chris Johnston), Джона Келси (John Kelsey), Ксуейа Лай (Xuejia Lai), Билла Лейнингера (Bill Leininger), Майка Марковица (Mike Markowitz), Ричарда Аутбриджа (Richard Outerbridge), Питера Пирсона (Peter Pearson), Кена Пиццини (Ken Pizzini), Кэлма Пламба (Calm Plumb), RSA Data Security, Inc., Майкла Роу (Michael Roe), Майкла Вуда (Michael Wood) и Фила Циммермана (Phil Zimmermann) — за предоставленные исходные коды; Пола МакНерланда (Paul MacNerland) — за создание рисунков к первому издания; Карен Купер (Karen Cooper) — за редактирование второго издания; Бота Фридмана (Both Friedman) — за сверку второго издания; Кэрол Кеннеди (Кэрол Kennedy) — за работу над предметным указателем для второго издания; читателей телеконференции `sci.crypt` и почтового списка Cypherpunks — за комментирование идей, ответы на вопросы и поиск ошибок в первом издании; Рэнди Сюсс (Randy Seuss) за предоставление доступа к Интернету; Джеффа Дантермана (Jeff Duntemann) и Джона Эриксона (Jon Erickson) — за то, что помогли мне начать; семью Инсли (Insley) (в произвольном порядке) — за стимуляцию, вдохновление, поддержку, беседы, дружбу и обеды; а также компанию AT&T Bell Labs, воодушевившую меня и сделавшей возможным все это. Все эти люди помогли написать намного более хорошую книгу, чем я мог бы создать в одиночку.

Брюс Шнайер