

# СОДЕРЖАНИЕ

<i>От издательства</i> .....	12
<i>Вступительное слово</i> .....	13
<i>Предисловие</i> .....	15
<i>Список аббревиатур</i> .....	19
<b>Глава 1. Шифрование</b> .....	22
Основы.....	23
Классические шифры.....	23
Шифр Цезаря.....	23
Шифр Виженера.....	24
Как работают шифры.....	25
Перестановка.....	26
Режим работы.....	27
Почему классические шифры небезопасны.....	28
Идеальное шифрование: одноразовый блокнот.....	29
Шифрование с помощью одноразового блокнота.....	29
Почему одноразовый блокнот безопасен?.....	30
Безопасность шифрования.....	32
Модели атак.....	32
Цели безопасности.....	35
Аспекты безопасности.....	36
Асимметричное шифрование.....	38
Дополнительные функции шифров.....	39
Шифрование с аутентификацией.....	39
Шифрование с сохранением формата.....	40
Полностью гомоморфное шифрование.....	41
Шифрование, допускающее поиск.....	41
Настраиваемое шифрование.....	41
Какие возможны проблемы.....	42
Слабый шифр.....	42
Неправильная модель.....	43
Для дополнительного чтения.....	44
<b>Глава 2. Случайность</b> .....	45
Случайное или неслучайное?.....	45
Случайность как распределение вероятностей.....	46
Энтропия: мера неопределенности.....	47
Генераторы случайных и псевдослучайных чисел.....	48

Как работает PRNG .....	49
Вопросы безопасности .....	50
PRNG Fortuna .....	51
Криптографически стойкие и нестойкие PRNG.....	52
Полезность статистических тестов.....	54
PRNG на практике .....	55
Генерирование случайных битов в системах на базе Unix.....	55
Функция CryptGenRandom() в Windows .....	59
Аппаратный PRNG: RDRAND в микропроцессорах Intel .....	60
Какие возможны проблемы.....	61
Плохие источники энтропии .....	61
Недостаточная энтропия на этапе начальной загрузки .....	61
Криптографически нестойкие PRNG .....	62
Дефектная выборка при стойком PRNG.....	63
Для дополнительного чтения.....	64
<b>Глава 3. Криптографическая безопасность.....</b>	<b>65</b>
Определение невозможного.....	66
Безопасность в теории: информационная безопасность .....	66
Безопасность на практике: вычислительная безопасность .....	66
Количественное измерение безопасности.....	68
Измерение безопасности в битах.....	68
Полная стоимость атаки .....	70
Выбор и вычисление уровней безопасности .....	71
Достижение безопасности .....	73
Доказуемая безопасность .....	73
Эвристическая безопасность .....	76
Генерирование ключей .....	77
Генерирование симметричных ключей.....	77
Генерирование асимметричных ключей.....	78
Защита ключей.....	79
Какие возможны проблемы.....	80
Ложное чувство безопасности.....	80
Короткие ключи для поддержки унаследованных приложений.....	80
Для дополнительного чтения.....	81
<b>Глава 4. Блочные шифры.....</b>	<b>82</b>
Что такое блочный шифр?.....	83
Цели безопасности .....	83
Размер блока.....	84
Атака по кодовой книге .....	84
Как устроены блочные шифры .....	85
Раунды блочного шифра.....	85
Сдвиговая атака и ключи раунда.....	86
Подстановочно-перестановочные сети .....	86
Схемы Фейстеля.....	87
Шифр Advanced Encryption Standard (AES).....	88

Внутреннее устройство AES .....	89
AES в действии .....	92
Реализация AES.....	92
Табличные реализации .....	93
Машинные команды .....	94
Безопасен ли AES? .....	95
Режимы работы.....	96
Режим электронной кодовой книги (ECB).....	96
Режим сцепления блоков шифртекста (CBC).....	98
Как зашифровать любое сообщение в режиме CBC .....	100
Режим счетчика (CTR).....	102
Какие возможны проблемы .....	104
Атаки типа встречи посередине.....	104
Атаки на оракул дополнения .....	106
Для дополнительного чтения.....	107
<b>Глава 5. Потокковые шифры</b> .....	108
Как работают потокковые шифры .....	109
Потокковые шифры с хранимым состоянием и на основе счетчика.....	110
Аппаратные потокковые шифры .....	111
Регистры сдвига с обратной связью.....	112
Grain-128a .....	119
A5/1.....	120
Программные потокковые шифры .....	123
RC4.....	124
Salsa20.....	129
Какие возможны проблемы.....	134
Повторное использование одноразового числа .....	134
Дефектная реализация RC4.....	135
Слабые аппаратно реализованные шифры.....	136
Для дополнительного чтения.....	137
<b>Глава 6. Функции хеширования</b> .....	138
Безопасные хеш-функции.....	139
И снова непредсказуемость .....	140
Стойкость к восстановлению прообраза.....	141
Стойкость к коллизиям .....	142
Нахождение коллизий.....	143
Построение функций хеширования .....	145
Хеш-функции на основе сжатия: построение Меркла–Дамгора .....	145
Хеш-функции на основе перестановок: функции губки .....	149
Семейство хеш-функций SHA .....	150
SHA-1 .....	151
SHA-2 .....	153
Конкурс на звание SHA-3.....	155
Кессак (SHA-3).....	156
Функция хеширования BLAKE 2 .....	158

Какие возможны проблемы.....	160
Атака удлинением сообщения.....	160
Обман протоколов доказательства хранения.....	161
Для дополнительного чтения.....	162

## **Глава 7. Хеширование с секретным ключом**.....163

Имитовставки (MAC) .....	164
MAC как часть безопасной системы связи .....	164
Атаки с подделкой и подобранным сообщением.....	164
Атаки повторным воспроизведением.....	165
Псевдослучайные функции (PRF).....	165
Безопасность PRF .....	166
Почему PRF более стойкие, чем MAC.....	166
Создание хешей с секретным ключом по хешам без ключа.....	167
Построение секретного префикса .....	167
Построение секретного суффикса .....	168
Построение HMAC .....	168
Обобщенная атака против MAC на основе функций хеширования.....	170
Создание функций хеширования на основе блочных шифров: CMAC .....	171
Взлом CBC-MAC.....	171
Исправление CBC-MAC.....	171
Проектирование специализированных имитовставок .....	173
Poly1305.....	173
SipHash .....	176
Какие возможны проблемы.....	178
Атаки с хронометражем на верификацию MAC.....	178
Когда губки протекают .....	180
Для дополнительного чтения.....	181

## **Глава 8. Шифрование с аутентификацией**.....182

Шифрование с аутентификацией с использованием MAC .....	183
Шифрование-и-MAC .....	183
MAC-затем-шифрование .....	184
Шифрование-затем-MAC.....	185
Шифры с аутентификацией.....	185
Шифрование с аутентификацией и ассоциированными данными .....	186
Предотвращение предсказуемости с помощью одноразовых чисел.....	187
Какой шифр с аутентификацией считать хорошим?.....	187
AES-GCM: стандартный шифр с аутентификацией.....	190
Внутреннее устройство GCM: CTR и GHASH .....	190
Безопасность GCM .....	192
Эффективность GCM.....	193
OCB: шифр с аутентификацией, более быстрый, чем GCM .....	193
Внутреннее устройство OCB .....	194
Безопасность OCB .....	194
Эффективность OCB.....	195
SIV: самый безопасный шифр с аутентификацией? .....	195

AEAD на основе перестановки .....	196
Какие возможны проблемы .....	198
AES-GCM и слабые хеш-ключи .....	198
AES-GCM и короткие жетоны .....	200
Для дополнительного чтения .....	201
<b>Глава 9. Трудные задачи</b> .....	<b>202</b>
Вычислительная трудность .....	203
Измерение времени работы .....	203
Полиномиальное и суперполиномиальное время .....	206
Классы сложности .....	207
Недетерминированное полиномиальное время .....	208
NP-полные задачи .....	209
Задача о равенстве P и NP .....	210
Задача факторизации .....	212
Факторизация больших чисел на практике .....	212
Является ли задача факторизации NP-полной? .....	214
Задача о дискретном логарифме .....	215
Что такое группа? .....	215
Трудная задача .....	216
Какие возможны проблемы .....	217
Когда разложить на множители легко .....	217
Небольшие трудные задачи трудными не являются .....	218
Для дополнительного чтения .....	219
<b>Глава 10. RSA</b> .....	<b>221</b>
Математические основания RSA .....	222
Перестановка с потайным входом в RSA .....	223
Генерирование ключей и безопасность RSA .....	224
Шифрование с помощью RSA .....	226
Взлом RSA-шифрования по учебнику и податливость .....	226
Стойкое RSA-шифрование: OAEP .....	226
Подписание с помощью RSA .....	228
Взлом RSA-подписей по учебнику .....	229
Стандарт цифровой подписи PSS .....	230
Подписи на основе полного хеша домена .....	231
Реализации RSA .....	232
Алгоритм быстрого возведения в степень .....	233
Выбор малых показателей степени для ускорения операций с открытым ключом .....	235
Китайская теорема об остатках .....	236
Какие возможны проблемы .....	238
Атака Bellcore на RSA-CRT .....	238
Разделение закрытых показателей степени или модулей .....	239
Для дополнительного чтения .....	240

<b>Глава 11. Протокол Диффи–Хеллмана</b> .....	242
Функция Диффи–Хеллмана .....	243
Проблемы протоколов Диффи–Хеллмана.....	245
Вычислительная задача Диффи–Хеллмана.....	245
Задача Диффи–Хеллмана о распознавании.....	246
Другие задачи Диффи–Хеллмана .....	246
Протоколы совместной выработки ключей.....	247
Пример протокола выработки ключа, не опирающегося на ДН.....	247
Модели атак на протоколы совместной выработки ключей.....	248
Производительность.....	250
Протоколы Диффи–Хеллмана .....	251
Анонимный протокол Диффи–Хеллмана.....	251
Протокол Диффи–Хеллмана с аутентификацией.....	253
Протокол Менезеса–Кью–Вэнстоуна.....	255
Какие возможны проблемы.....	257
Пренебрежение хешированием разделяемого секрета .....	257
Унаследованный протокол Диффи–Хеллмана в TLS .....	258
Небезопасные параметры группы .....	258
Для дополнительного чтения.....	258
<b>Глава 12. Эллиптические кривые</b> .....	260
Что такое эллиптическая кривая? .....	261
Эллиптические кривые над множеством целых чисел .....	262
Сложение и умножение точек .....	264
Группы эллиптических кривых.....	267
Задача ECDLP.....	268
Протокол совместной выработки ключа Диффи–Хеллмана над эллиптическими кривыми .....	269
Подписание с помощью эллиптических кривых.....	270
Шифрование с помощью эллиптических кривых .....	272
Выбор кривой .....	273
Кривые, рекомендованные NIST .....	274
Кривая Curve25519 .....	275
Другие кривые .....	275
Какие возможны проблемы.....	276
ECDSA с недостаточной случайностью .....	276
Взлом ECDH с помощью другой кривой .....	276
Для дополнительного чтения.....	277
<b>Глава 13. Протокол TLS</b> .....	278
Целевые приложения и требования .....	279
Набор протоколов TLS.....	280
Семейство протоколов TLS и SSL: краткая история.....	280
TLS в двух словах .....	281
Сертификаты и удостоверяющие центры .....	281
Протокол записи .....	284

Протокол подтверждения связи.....	285
Криптографические алгоритмы TLS 1.3 .....	287
Улучшения TLS 1.3 по сравнению с TLS 1.2 .....	288
Защита от понижения версии.....	289
Квитирование с одним периодом кругового обращения .....	289
Возобновление сеанса .....	289
Стойкость TLS.....	290
Аутентификация .....	290
Секретность прошлого .....	291
Какие возможны проблемы .....	292
Скомпрометированный удостоверяющий центр.....	292
Скомпрометированный сервер.....	292
Скомпрометированный клиент .....	293
Дефекты реализации .....	293
Для дополнительного чтения.....	294
<b>Глава 14. Квантовая и постквантовая криптография .....</b>	<b>295</b>
Как работают квантовые компьютеры.....	296
Квантовые биты .....	297
Квантовые вентили .....	299
Квантовое ускорение.....	302
Экспоненциальное ускорение и задача Саймона.....	302
Угроза со стороны алгоритма Шора.....	303
Решение задачи факторизации с помощью алгоритма Шора.....	304
Алгоритм Шора и задача о дискретном логарифме .....	305
Алгоритм Гровера.....	305
Почему так трудно построить квантовый компьютер? .....	306
Постквантовые криптографические алгоритмы.....	308
Криптография на основе кодов.....	308
Криптография на основе решеток.....	309
Криптография на основе многомерных систем .....	310
Криптография на основе функций хеширования .....	312
Какие возможны проблемы .....	313
Непонятный уровень безопасности.....	313
Забегаая вперед: что, если уже слишком поздно?.....	314
Проблемы реализации .....	315
Для дополнительного чтения.....	315
<b>Предметный указатель .....</b>	<b>317</b>

## От издательства

### **Отзывы и пожелания**

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте [www.dmkpress.com](http://www.dmkpress.com), зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com); при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу [http://dmkpress.com/authors/publish\\_book/](http://dmkpress.com/authors/publish_book/) или напишите в издательство по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com).

### **Скачивание исходного кода примеров**

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте [www.dmkpress.com](http://www.dmkpress.com) на странице с описанием соответствующей книги.

### **Список опечаток**

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу [dmkpress@gmail.com](mailto:dmkpress@gmail.com). Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

### **Нарушение авторских прав**

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и No Starch Press очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты [dmkpress@gmail.com](mailto:dmkpress@gmail.com).

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.



# ВСТУПИТЕЛЬНОЕ СЛОВО

Если вы читали какие-нибудь книги по компьютерной безопасности, то, наверное, встречались с распространенным взглядом на криптографию. «Криптография, – говорят авторы, – самое прочное звено в цепочке». Оценка похвальная, но не вполне точная. Если криптография – действительно самая прочная часть системы, то зачем тратить время на ее улучшение, когда есть много других частей, нуждающихся во внимании?

И если попытаться сформулировать главный урок, который я хочу преподать этой книгой, то он состоит в том, что такой взгляд на криптографию, мягко говоря, идеализирован, а по сути является мифом. Криптография прочна *в теории*, а на практике столь же подвержена ошибкам, как и любой другой аспект системы безопасности. Особенно это относится к случаям, когда криптографическую систему реализуют непрофессионалы, не имеющие достаточного опыта и пренебрегающие деталями, – а таковы многие развернутые в настоящее время системы. Хуже того – если реализация криптографической системы содержит ошибки, то проявления их зачастую оказываются весьма скандальными.

Но какое вам до этого дело, и зачем нужна эта книга?

Когда почти двадцать лет назад я только начинал заниматься прикладной криптографией, разработчикам ПО была доступна лишь отрывочная и не самая актуальная информация. Криптографы придумывали алгоритмы и протоколы, а программисты, реализовывая их, создавали запутанные, плохо документированные библиотеки, пред-

назначенные в первую очередь для других специалистов. Существовало – и до сих пор существует – глубокая пропасть между теми, кто знает и понимает криптографические алгоритмы, и теми, кто этими алгоритмами пользуется (или на свой страх и риск пренебрегает ими). На рынке имеется очень немного достойных книг, и еще меньше полезных программисту-практику.

Результаты такого положения удручают. Я имею в виду факты компрометации, о которых говорят такие ярлыки, как «CVE» или «Серьезность: высокая», а в некоторых особо тревожных ситуациях – атаки, которые на слайдах снабжены грифом «СОВЕРШЕННО СЕКРЕТНО». Если вам и известны некоторые особо знаменитые примеры, то только потому, что они затрагивают системы, от которых зависит ваша работа. Многие проблемы подобного рода возникают, потому что криптография – сложная и математически элегантная теория, а специалисты по ней не потрудились поделиться знаниями с инженерами, которые пишут программный код.

По счастью, ситуация начинает меняться, и пример тому – эта книга.

Книга «О криптографии всерьез» написана одним из самых известных экспертов по прикладной криптографии, однако ориентирована не на других специалистов того же профиля. Но и поверхностным обзором этой дисциплины она тоже не является. Напротив, она содержит скрупулезное и современное обсуждение криптографической техники, призванное помочь стать лучше практикам, собирающимся подвизаться в этой области. Вы узнаете не только о том, как работают алгоритмы, но и как использовать их в реальных системах.

Изложение начинается с рассмотрения основных криптографических примитивов, в т. ч. блочных шифров, схем шифрования с открытым ключом, функций хеширования и генераторов случайных чисел. В каждой главе приводятся примеры работы алгоритмов и объясняется, что следует и чего *не* следует делать. В последних главах рассматриваются темы повышенной трудности, например TLS, а также будущее криптографии – что делать после того, как придут квантовые компьютеры и усложнят нам жизнь.

Конечно, одна книга не в состоянии решить все наши проблемы, но знания накапливаются по крупицам. В этой книге таких крупиц много. Быть может, даже достаточно для того, чтобы развернутые на практике криптографические системы стали, наконец, соответствовать тем высоким требованиям, которые к ним предъявляются.

Полезного вам чтения.

Мэттью Д. Грин,  
профессор Института информационной безопасности  
университета Джонса Хопкинса

# ПРЕДИСЛОВИЕ



Я написал книгу, которую хотел бы иметь, когда только начал изучать криптографию. В 2005 году под Парижем я учился в магистратуре и с предвкушением записался на спецкурс по криптографии. Увы, спецкурс был отменен, потому что не набралось достаточного количества желающих. «Криптография – это слишком сложно», – говорили студенты и массово записывались на курсы по компьютерной графике и базам данных.

С тех пор слова «криптография – это сложно» я слышал неоднократно. Но так ли сложна криптография в действительности? Чтобы играть на музыкальном инструменте, овладеть языком программирования или воплотить на практике достижения какой-нибудь увлекательной дисциплины, необходимо изучить определенные концепции и символы, но для этого необязательно иметь докторскую степень. Я думаю, что это относится и к желанию стать компетентным криптографом. А также полагаю, что криптография считается такой трудной наукой, потому что криптографы не приложили достаточных усилий к ее преподаванию.

И есть еще одна причина, по которой я считаю эту книгу необходимой: криптография превратилась в довольно разветвленную область знаний. Чтобы сделать что-то полезное и важное в криптографии, нужно разбираться в смежных областях: как работают компьютеры и сети, что нужно пользователям и системам и как противник может злонамеренно воспользоваться алгоритмами и их реализациями. Иными словами, необходима связь с реальностью.

## Подход, принятый в этой книге

Первоначально книга называлась «Crypto for Real», чтобы подчеркнуть практически ориентированный, деловой подход, которому я намеревался следовать. Я хотел не столько опростить криптографию, сколько связать с ее с реальными приложениями. Я привожу примеры исходного кода и описываю реальные ошибки и кошмарные истории.

Помимо четкой связи с реальностью, в основу книги положены еще два краеугольных камня: простота и современность. Упрощаю я изложение только по форме, не жертвуя содержанием: представляю много нетривиальных идей, но без скучного математического формализма. Я хочу, чтобы читатель понял основополагающие идеи криптографии, это кажется мне важнее, чем запоминание бесконечных формул. Что касается современности, то я рассматриваю последние теоретические результаты и приложения, например протокол TLS 1.3 и криптографию в постквантовую эпоху. Я не обсуждаю детали устаревших или небезопасных алгоритмов, например DES или MD5. Исключением является алгоритм RC4, но и он включен только для того, чтобы продемонстрировать, в чем его слабость и как работают потоковые шифры такого рода.

Книга «Криптография всерьез» не является ни путеводителем по криптографическому программному обеспечению, ни сводом технических спецификаций – такие вещи легко найти в сети. Ее главное назначение – пробудить у вас интерес к криптографии и попутно рассказать о ее фундаментальных концепциях.

## Для кого предназначена эта книга

Во время работы над книгой я часто представлял себе читателя как разработчика, который оказался вынужден иметь дело с криптографией, но так и остался в растерянности после чтения заумных учебников и научных статей. Разработчики часто должны – и хотят – лучше понимать криптографию, чтобы избежать неудачных проектных решений, и я надеюсь, что в этом моя книга поможет.

Но если вы не являетесь разработчиком, тоже ничего страшного! Чтение книги не потребует от вас владения навыками кодирования, она доступна любому, кто знаком с основами информатики и математикой в объеме технического вуза (начала теории вероятностей, арифметики по модулю и т. д.).

Но, несмотря на сравнительную доступность книги, для получения от нее максимальной пользы все же требуется приложить некоторые усилия. Мне приходит на ум аналогия с альпинизмом: автор прокладывает путь, снабжает вас веревками и ледорубом, но покорить гору вам придется самостоятельно. Изучение изложенных в книге идей потребует труда, но в конце преодолевшего все препятствия ждет награда.

## Структура книги

Книга состоит из четырнадцати глав, разбитых на четыре части. По большей части главы независимы, за исключением главы 9, в которой заложен фундамент для трех последующих глав. Но я все же рекомендую сначала прочитать первые три главы.

### Основы

- **Глава 1 «Шифрование».** Здесь вводится понятие безопасного шифрования, начиная со слабых шифров с использованием карандаша и бумаги и заканчивая стойкими рандомизированными шифрами.
- **Глава 2 «Случайность».** Описывается, как работает генератор псевдослучайных чисел, когда такой генератор считается безопасным и как его безопасно использовать.
- **Глава 3 «Криптографическая безопасность».** Обсуждается теоретическая и практическая безопасность, сравнивается предположительная и доказуемая безопасность.

### Симметричные криптографические системы

- **Глава 4 «Блочные шифры».** Рассматриваются шифры, обрабатывающие сообщения поблочно. Основное внимание уделяется самому известному из них, Advanced Encryption Standard (AES).
- **Глава 5 «Потоковые шифры».** Описываются шифры, порождающие поток случайных на первый взгляд битов, которые объединяются с сообщением операцией XOR.
- **Глава 6 «Функции хеширования».** Функции хеширования – чуть ли не единственный алгоритм, не нуждающийся в секретном ключе, и при этом один из самых распространенных строительных блоков в криптографии.
- **Глава 7 «Хеширование с секретным ключом».** Объясняется, что будет, если соединить функцию хеширования с секретным ключом, и как этим можно воспользоваться для аутентификации сообщений.
- **Глава 8 «Шифрование с аутентификацией».** На примерах описываются алгоритмы, которые могут одновременно зашифровать и аутентифицировать сообщение, в частности стандарт AES-GCM.

### Асимметричные криптографические системы

- **Глава 9 «Трудные задачи».** Здесь заложен теоретический фундамент шифрования с открытым ключом; используется нотация из теории вычислительной сложности.
- **Глава 10 «RSA».** В алгоритме RSA задача разложения на множители применяется для построения схем безопасного шифрования и цифровой подписи с помощью простых арифметических операций.

- **Глава 11 «Протокол Диффи–Хеллмана».** Идея асимметричной криптографии обобщается на понятие совместной выработки ключей, когда две стороны вырабатывают секретное значение, используя только несекретные данные.
- **Глава 12 «Эллиптические кривые».** Простое введение в эллиптическую криптографию – самый быстрый вид асимметричных криптографических систем.

## Приложения

- **Глава 13 «Протокол TLS».** Рассматривается протокол Transport Layer Security (TLS), пожалуй, самый важный для безопасности сетей.
- **Глава 14 «Квантовая и постквантовая криптография».** В этой заключительной главе с оттенком научной фантастики обсуждаются квантовые вычисления и новый вид криптографии.

## Благодарности

Хочу поблагодарить Яна, Энни и других сотрудников издательства No Starch, принявших участие в подготовке этой книги, а особенно Билла, который поверил в проект с самого начала, терпеливо усваивал трудные темы и превращал мои беспорядочные черновики в читаемый текст. Я также благодарен Лорел, которая вносила мои многочисленные поправки и благодаря которой книга выглядит так симпатично.

Что касается технической стороны, то книга содержала бы куда больше ошибок и неточностей, если бы не помощь следующих лиц: Джон Каллас, Билл Кокс, Нильс Фергюсон, Филипп Йованович, Сэмюэл Нивс, Дэвид Рейд, Филлип Рогузэй, Эрик Тьюз, – а также читателей предварительной версии, сообщавших о найденных ошибках. Наконец, я благодарю Мэтта Грина, написавшего вступительное слово.

Я также выражаю благодарность своему работодателю, компании Kudelski Security, выделившей мне время для работы над книгой. Наконец, моя глубочайшая благодарность Александре и Мелине за поддержку и терпение.

Лозанна, 17.05.2017 (три простых числа)

# СПИСОК АББРЕВИАТУР

AE	authenticated encryption (шифрование с аутентификацией)
AEAD	authentication encryption with associated data (шифрование с аутентификацией и ассоциированными данными)
AES	Advanced Encryption Standard (улучшенный стандарт шифрования)
AES-NI	AES native instructions (AES с платформенными командами)
AKA	authenticated key agreement (совместная выработка ключей с аутентификацией)
API	application program interface (интерфейс прикладной программы)
ARX	add-rotate-XOR
ASIC	application-specific integrated circuit (специализированная заказная интегральная схема)
CA	certificate authority (удостоверяющий центр, УЦ)
CAESAR	Конкурс шифрования с аутентификацией: безопасность, применимость и надежность
CBC	cipher block chaining (режим сцепления блоков шифртекста)
CCA	chosen-ciphertext attack (атака с подобранным шифртекстом)
CDH	computational Diffie–Hellman (предположение о вычислительной трудности задачи Диффи–Хеллмана)
CMAC	cipher-based MAC (имитовставка на основе блочного шифра)
COA	ciphertext-only attack (атака на основе шифртекста)
CPA	chosen-plaintext attack (атака с подобранным открытым текстом)
CRT	Chinese remainder theorem (китайская теорема об остатках)
CTR	режим счетчика
CVP	closest vector problem (задача о ближайшем векторе)
DDH	decisional Diffie–Hellman (предположение Диффи–Хеллмана о распознавании)

DES	Data Encryption Standard (стандарт шифрования данных)
DH	Diffie–Hellman
DLP	discrete logarithm problem (задача дискретного логарифмирования)
DRBG	deterministic random bit generator (детерминированный генератор случайных битов)
ECB	electronic codebook (режим электронной кодовой книги)
ECC	elliptic curve cryptography (эллиптическая криптография)
ECDH	elliptic curve Diffie–Hellman (эллиптический метод Диффи–Хеллмана)
ECDLP	elliptic-curve discrete logarithm problem (задача дискретного логарифмирования на эллиптической кривой)
ECDSA	elliptic-curve digital signature algorithm (алгоритм цифровой подписи на эллиптической кривой)
FDH	Full Domain Hash (полный хеш домена)
FHE	fully homomorphic encryption (полностью гомоморфное шифрование)
FIPS	Federal Information Processing Standards (Федеральный стандарт обработки информации)
FPE	format-preserving encryption (шифрование с сохранением формата)
FPGA	field-programmable gate array (программируемая пользователем вентиляционная матрица, ППВМ)
FSR	feedback shift register (регистр сдвига с обратной связью)
GCD	greatest common divisor (наибольший общий делитель, НОД)
GCM	Galois Counter Mode (режим счетчика с аутентификацией Галуа)
GNFS	general number field sieve (общий метод решета числового поля)
HKDF	HMAC-based key derivation function (функция формирования ключа на основе HMAC)
HMAC	hash-based message authentication code (имитовставка на основе функции хеширования)
HTTPS	HTTP Secure (безопасный HTTP)
IND	indistinguishability (неразличимость)
IP	Internet Protocol
IV	initial value (начальное значение)
KDF	key derivation function (функция формирования ключа)
KPA	known-plaintext attack (атака с известным простым текстом)
LFSR	linear feedback shift register (линейный регистр сдвига с обратной связью)
LSB	least significant bit (младший бит)
LWE	learning with errors (обучение с ошибками)
MAC	message authentication code (имитовставка)
MD	message digest (дайджест сообщения)
MitM	meet-in-the-middle (метод встречи посередине)
MQ	multivariate quadratics (многомерные системы квадратичных уравнений)
MQV	Menezes–Qu–Vanstone (протокол Менезеса–Кью–Вэнстоуна)
MSB	most significant bit (старший бит)



MT	Mersenne Twister (вихрь Мерсенна)
NFSR	nonlinear feedback shift register (нелинейный регистр сдвига с обратной связью)
NIST	National Institute of Standards and Technology (Национальный институт стандартов и технологий)
NM	non-malleability (неподатливость)
OAEP	Optimal Asymmetric Encryption Padding (оптимальное асимметричное шифрование с дополнением)
OCB	offset codebook (режим кодовой книги со смещением)
P	polynomial time (полиномиальное время)
PLD	programmable logic device (программируемое логическое устройство)
PRF	pseudorandom function (псевдослучайная функция)
PRNG	pseudorandom number generator (генератор псевдослучайных чисел)
PRP	pseudorandom permutation (псевдослучайная перестановка)
PSK	pre-shared key (предварительно разделенный ключ)
PSS	Probabilistic Signature Scheme (вероятностная схема подписи)
QR	quarter-round (четверть раунда)
QRNG	quantum random number (квантовый генератор случайных чисел)
RFC	request for comments (запрос на комментарии)
RNG	random number generator (генератор случайных чисел)
RSA	Rivest–Shamir–Adleman (алгоритм Ривеста–Шамира–Адлемана)
SHA	Secure Hash Algorithm (безопасный алгоритм хеширования)
SIS	short integer solution (короткое целочисленное решение)
SIV	synthetic IV (синтетическое начальное значение)
SPN	substitution–permutation network (подстановочно-перестановочная сеть)
SSH	Secure Shell (безопасная оболочка)
SSL	Secure Socket Layer (уровень безопасных сокетов)
TE	tweakable encryption (настраиваемое шифрование)
TLS	Transport Layer Security (безопасность транспортного уровня)
TMTO	time-memory trade-off (компромисс между временем и памятью)
UDP	User Datagram Protocol (протокол пользовательских дейтаграмм)
UH	universal hash (универсальная функция хеширования)
WEP	Wired Equivalent Privacy (протокол безопасности в беспроводных сетях)
WOTS	Winternitz one-time signature (одноразовая подпись Винтерница)
XOR	exclusive OR (исключающее ИЛИ)

# 1

## ШИФРОВАНИЕ



Шифрование – главное применение криптографии; его цель – сделать данные непонятными и тем самым обеспечить их *конфиденциальность*. Для шифрования используется алгоритм, называемый *шифром*, и секретное значение, называемое *ключом*; не зная секретного ключа, невозможно получить ни одного бита зашифрованного сообщения, не говоря уже о том, чтобы его дешифровать.

В данной главе предметом нашего внимания будет *симметричное шифрование*, его простейшая разновидность. В этом случае для дешифрования используется тот же ключ, что для шифрования (в отличие от *асимметричного шифрования*, или *шифрования с открытым ключом*, когда ключи шифрования и дешифрования различны). Мы начнем с рассмотрения самых слабых форм симметричного шифрования – классических шифров, способных устоять только перед совсем необразованным противником, а затем перейдем к самым стойким шифрам, взломать которые вообще невозможно.

# ОСНОВЫ

В контексте шифрования *открытым текстом* называется незашифрованное сообщение, а *шифртекстом* – зашифрованное сообщение. Шифр состоит из двух функций: *шифрование* преобразует открытый текст в шифртекст, а *дешифрирование* производит обратное преобразование шифртекста в открытый. Но часто говорят «шифр», имея в виду «шифрование». Например, на рис. 1.1 показан шифр **E**, представленный прямоугольником, который принимает открытый текст *P* и ключ *K* и порождает на выходе шифртекст *C*. Я буду записывать это соотношение в виде  $C = E(K, P)$ . Аналогично, когда шифр работает в режиме дешифрирования, я буду писать  $D(K, C)$ .

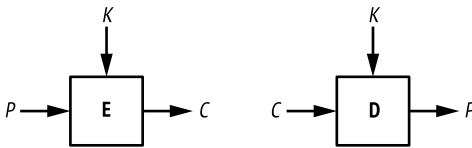


Рис. 1.1. Простейшее шифрование и дешифрирование

**Примечание** Для некоторых шифров размер шифртекста равен размеру открытого текста, для других он немного больше. Но никогда шифртекст не может быть короче открытого текста.

## Классические шифры

Классическими называются шифры, появившиеся раньше компьютеров и потому применяемые к буквам, а не к битам. Они гораздо проще современных шифров типа DES – например, в Древнем Риме или во время Первой мировой войны для шифрования сообщения нельзя было воспользоваться всей мощностью компьютера, так что приходилось довольствоваться бумагой и карандашом. Существует много классических шифров, но наиболее известны шифры Цезаря и Виженера.

### Шифр Цезаря

Шифр Цезаря назван так, потому что, согласно древнеримскому историку Светонию, им пользовался Юлий Цезарь. Сообщение шифруется путем сдвига каждой буквы на три позиции вправо по алфавиту с оборотом по достижении Z. Например, ZOO шифруется как CRR, результатом дешифрирования FDHVDU является CAESAR и т. д., как показано на рис. 1.2. В числе 3 нет ничего особенного, просто так производить вычисления в уме проще, чем при выборе, скажем, 11 или 23.

Взломать шифр Цезаря проще простого: чтобы дешифрировать заданный шифртекст, нужно просто сдвинуть каждую букву на три позиции влево. Однако шифр Цезаря, наверное, был достаточно стойким во времена Красса и Цицерона. Поскольку никакого секретного ключа нет

(он всегда равен 3), пользователи шифра Цезаря должны были считать, что противник тупой и не знает, как его найти, – такое предположение в наши дни выглядит совсем уж нереалистично. (Правда, в 2006 году итальянская полиция арестовала босса мафии, расшифровав сообщения, написанные на клочках бумаги с использованием варианта шифра Цезаря; например, ABC было зашифровано как 456, а не DEF.)

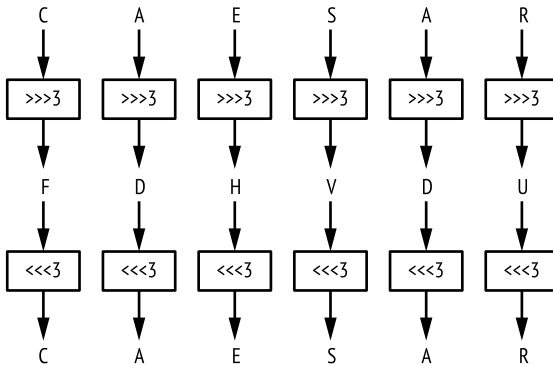


Рис. 1.2. Шифр Цезаря

Можно ли сделать шифр Цезаря более безопасным? Например, можно было сдвигать не на 3, а на какое-нибудь секретное значение, но это не спасало бы положения, потому что противнику достаточно было бы перебрать все 25 возможных значений сдвига и найти то, при котором расшифрованное сообщение становится осмысленным.

## Шифр Виженера

Для существенного улучшения шифра Цезаря потребовалось примерно 1500 лет, в XVI веке итальянец Джовани Баттиста Белассо создал шифр Виженера. Имя «Виженер» принадлежит французу Блезу де Виженеру, который изобрел в XVI веке другой шифр, но из-за неправильной атрибуции вошел в историю. Так или иначе, шифр Виженера обрел популярность и использовался, в частности, конфедератами во время Гражданской войны в США и швейцарской армией во время Первой мировой войны.

Шифр Виженера похож на шифр Цезаря, только величина сдвига составляет не три позиции, а определяется *ключом*, набором букв, которым соответствуют числа, равные позиции буквы в алфавите. Например, если ключ равен DУН, то буквы открытого текста сдвигаются на 3, 20 и 7 позиций, потому что D отстоит от А на три позиции, U – на 20 позиций, а H – на семь позиций. Последовательность 3, 20, 7 повторяется, пока не будет зашифрован весь открытый текст. Например, слово CRYPTO на ключе DУН было бы зашифровано как FLFSNV: C сдвигается на три позиции и превращается в F, R сдвигается на 20 и превращается в L и т. д. На рис. 1.3 показано, как этот принцип применяется к шифрованию предложения THEY DRINK THE TEA.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

[e-Univers.ru](http://e-Univers.ru)