Реальная криптография

Дэвид Вонг

ПИТЕР®

Санкт-Петербург • Москва • Минск

2025

Краткое содержание

Предисловие 16

Благодарности 21

О книге 22

Об авторе 27

Иллюстрация на обложке 28

Часть I. Примитивы: криптографические ингредиенты

Глава 1. Введение 31

Глава 2. Хеш-функции 55

Глава 3. Имитовставки 80

Глава 4. Аутентифицированное шифрование 98

Глава 5. Обмен ключами 124

Глава 6. Асимметричный и гибридный виды шифрования 148

Глава 7. Подписи и доказательства с нулевым разглашением 171

Глава 8. Случайность и секреты 196

Часть II. Протоколы: рецепты применения криптографии

Глава 9. Безопасная передача данных 223

Глава 10. Сквозное шифрование. 251

Глава 11. Аутентификация пользователей 280

Глава 12. Криптография и криптовалюты. 309

Глава 13. Аппаратная криптография 338

Глава 14. Постквантовая криптография 362

Глава 15. Криптография следующего поколения 389

Глава 16. Условия, в которых криптография может не сработать 415

Приложение. Ответы к упражнениям 429

Оглавление

Предисловие 16
Книга, которая создавалась много лет 16
Реальный учебный план для криптографов 17
Где находится большинство ошибок 18
Нужно ли было писать еще одну книгу? 19

Благодарности 21

О книге 22
Кому следует прочитать книгу 22
Студенты 22
Практикующие специалисты 22
Разработчики, прямо или косвенно использующие криптографию 23
Криптографы, интересующиеся другими областями 23
Инженеры и менеджеры по продуктам, желающие лучше разобраться в теме 23
Люди, которые хотят узнать о криптографии, применяемой в реальной жизни 23
Уровень подготовки читателя 24
Как организована книга 24
Примеры исходного кода 26
От издательства 26

Об авторе 27

Иллюстрация на обложке 28

Часть I. Примитивы: криптографические ингредиенты

Глава 1. Введение 31
1.1. Криптография как защита протоколов 32
1.2. Симметричная криптография. Что такое симметричное шифрование . . . 33
1.3. Принцип Керкгоффса: секретом является только ключ. 35
1.4. Асимметричная криптография: два ключа лучше одного. 38
1.4.1. Обмен ключами, или Как получить общий секрет 38
1.4.2. Асимметричное шифрование, не похожее на симметричное 40
1.4.3. Цифровые подписи, прямо как подписи на бумаге 43
1.5. Классификация и обобщение в области криптографии 45
1.6. Криптография в теории и криптография реального мира 47
1.7. От теории к практике: выбери себе приключение 48
1.8. Предупреждение 53
Резюме 54

Глава 2. Хеш-функции 55
2.1. Что такое хеш-функция. 55
2.2. Свойства безопасности хеш-функции 58
2.3. Методы обеспечения безопасности для хеш-функций 61
2.4. Хеш-функции на практике 62
2.4.1. Обязательства 63
2.4.2. Целостность субресурсов 63
2.4.3. BitTorrent 64
2.4.4. Tor 64
2.5. Стандартизированные хеш-функции 65
2.5.1. Хеш-функция SHA-2 66
2.5.2. Хеш-функция SHA-3 69
2.5.3. SHAKE и cSHAKE — две функции расширенного выхода (XOF) . . 73
2.5.4. Избегание неоднозначного хеширования с помощью TupleHash 75
2.6. Хеширование паролей. 77
Резюме 79

Глава 3. Имитовставки 80
3.1. Файлы cookie без сохранения состояния: поясняющий пример имитовставок 81
3.2. Пример с кодом 84
3.3. Свойства безопасности имитовставки. 85
3.3.1. Подделка аутентификационного тега 85
3.3.2. Длина аутентификационного тега. 86
3.3.3. Атаки повторного воспроизведения 87
3.3.4. Проверка аутентификационных тегов за постоянное время 88
3.4. Имитовставка в реальном мире 90
3.4.1. Аутентификация сообщения 90
3.4.2. Получение ключей 90

3.4.3. Целостность файлов cookie . . . 91
3.4.4. Хеш-таблицы . . . 91
3.5. Практическое использование имитовставок . . . 91
3.5.1. HMAC — имитовставка с использованием хеш-функции . . . 92
3.5.2. KMAC — имитовставка с использованием cSHAKE . . . 93
3.6. SHA-2 и атаки удлинением сообщения . . . 94
Резюме . . . 97

Глава 4. Аутентифицированное шифрование . . . 98
4.1. Что такое шифр . . . 99
4.2. Блочный шифр Advanced Encryption Standard . . . 101
4.2.1. Какой уровень криптостойкости обеспечивает AES . . . 101
4.2.2. Интерфейс AES . . . 102
4.2.3. Внутренняя структура AES . . . 103
4.3. Зашифрованный пингвин и режим сцепления блоков шифротекста . . . 105
4.4. Отсутствие подлинности и решение проблемы в виде AES-CBC-HMAC . . . 108
4.5. Комплексные конструкции. Аутентифицированное шифрование . . . 110
4.5.1. Что такое аутентифицированное шифрование с присоединенными данными . . . 110
4.5.2. AEAD-алгоритм AES-GCM . . . 112
4.5.3. ChaCha20Poly1305 . . . 117
4.6. Другие виды симметричного шифрования . . . 121
4.6.1. Обертка ключа . . . 121
4.6.2. Аутентифицированное шифрование, устойчивое к некорректному применению nonce . . . 121
4.6.3. Шифрование диска . . . 122
4.6.4. Шифрование базы данных . . . 122
Резюме . . . 123

Глава 5. Обмен ключами . . . 124
5.1. Что такое обмен ключами . . . 125
5.2. Алгоритм обмена ключами Диффи — Хеллмана . . . 128
5.2.1. Теория групп . . . 128
5.2.2. Задача дискретного логарифма — основа алгоритма Диффи — Хеллмана . . . 132
5.2.3. Стандарты, описывающие алгоритм Диффи — Хеллмана . . . 134
5.3. Алгоритм обмена ключами Диффи — Хеллмана на эллиптических кривых . . . 136
5.3.1. Что такое эллиптические кривые . . . 136
5.3.2. Как работает протокол обмена ключами Диффи — Хеллмана на эллиптических кривых . . . 140
5.3.3. Стандарты, описывающие алгоритм Диффи — Хеллмана на эллиптических кривых . . . 142
5.4. Атаки через малые подгруппы и другие аспекты безопасности . . . 143
Резюме . . . 147

Глава 6. Асимметричный и гибридный виды шифрования 148
6.1. Что такое асимметричное шифрование 149
6.2. Практическое применение асимметричного шифрования и гибридное шифрование 151
6.2.1. Обмен ключами и инкапсуляция ключа 151
6.2.2. Гибридное шифрование 152
6.3. Асимметричное шифрование посредством алгоритма RSA: большее и меньшее зло 157
6.3.1. Классический алгоритм RSA 157
6.3.2. Почему не стоит использовать RSA PKCS#1 v1.5 162
6.3.3. Асимметричное шифрование с помощью RSA-OAEP 164
6.4. Гибридное шифрование с помощью алгоритма ECIES 167
Резюме 170

Глава 7. Подписи и доказательства с нулевым разглашением 171
7.1. Что такое подпись 172
7.1.1. Как на практике происходит добавление и проверка подписи 173
7.1.2. Основной пример применения подписей — аутентифицированный обмен ключами 174
7.1.3. Использование подписей в реальном мире. Инфраструктура открытых ключей 175
7.2. Доказательства с нулевым разглашением. Происхождение подписей . . . 176
7.2.1. Протокол идентификации Шнорра — интерактивное доказательство с нулевым разглашением 177
7.2.2. Подписи как неинтерактивные доказательства с нулевым разглашением 180
7.3. Алгоритмы подписи, которые следует (или не стоит) использовать 181
7.3.1. Плохой стандарт RSA PKCS#1 v1.5 182
7.3.2. Лучший стандарт RSA-PSS 185
7.3.3. Алгоритм цифровой подписи на эллиптических кривых 186
7.3.4. Алгоритм цифровой подписи на кривой Эдвардса 188
7.4. Тонкости схем подписи 192
7.4.1. Атаки на подписи через подмену 192
7.4.2. Деформируемость подписи 194
Резюме 194

Глава 8. Случайность и секреты 196
8.1. Что такое случайность 197
8.2. Медленная генерация случайности? На помощь придет генератор псевдослучайных чисел 199
8.3. Генерация случайности на практике 203
8.4. Генерация случайности и требования обеспечения безопасности 205
8.5. Открытая случайность 208
8.6. Формирование ключей с помощью HKDF 210
8.7. Управление ключами и секретами 214
8.8. Децентрализация доверия с помощью пороговой криптографии 216
Резюме 220

Часть II. Протоколы: рецепты применения криптографии

Глава 9. Безопасная передача данных 223
9.1. Протоколы SSL и TLS 223
9.1.1. От SSL к TLS 224
9.1.2. Практическое применение протокола TLS 225
9.2. Принцип работы протокола TLS 227
9.2.1. TLS-рукопожатие 228
9.2.2. Шифрование данных приложения с помощью протокола TLS 1.3 242
9.3. Современное состояние зашифрованного веба 243
9.4. Другие безопасные транспортные протоколы 246
9.5. Протокольный фреймворк Noise — современная альтернатива TLS 247
9.5.1. Схемы рукопожатия фреймворка Noise 247
9.5.2. Процесс рукопожатия при использовании фреймворка Noise 248
Резюме 250

Глава 10. Сквозное шифрование 251
10.1. Зачем нужно сквозное шифрование 252
10.2. Корня доверия нигде не найти 254
10.3. Провалы в сфере шифрования электронной почты 255
10.3.1. PGP или GPG? И как все это работает 255
10.3.2. Масштабирование доверия между пользователями с помощью сети доверия 259
10.3.3. Обнаружение ключей — это настоящая проблема 260
10.3.4. Если не PGP, то что? 262
10.4. Безопасный обмен сообщениями. Современный взгляд на сквозное шифрование на примере протокола Signal 263
10.4.1. Большее удобство для пользователя по сравнению с WOT: доверяй, но проверяй 265
10.4.2. X3DH — рукопожатие в рамках протокола Signal 267
10.4.3. Двойной храповик — протокол Signal, используемый после рукопожатия 271
10.5. Текущее состояние области сквозного шифрования 276
Резюме 279

Глава 11. Аутентификация пользователей 280
11.1. Краткий обзор темы аутентификации 281
11.2. Аутентификация пользователей, или Попытка избавиться от паролей 283
11.2.1. Один пароль для всего. Технология единого входа и менеджеры паролей 285
11.2.2. Не хотите видеть их пароли? Используйте асимметричный обмен ключами с парольной аутентификацией 287
11.2.3. Одноразовые пароли — это не совсем пароли: беспарольная аутентификация с симметричными ключами 291
11.2.4. Замена паролей асимметричными ключами 295

11.3. Аутентификация, управляемая пользователем, — сопряжение устройств при участии человека . . . 298
11.3.1. Предварительно распределенные ключи . . . 300
11.3.2. Симметричный обмен ключами с парольной аутентификацией с протоколом CPace . . . 302
11.3.3. Чтобы проверить, не подвергся ли ваш обмен ключами атаке посредника, используйте короткую аутентификационную строку . . . 303
Резюме . . . 307

Глава 12. Криптография и криптовалюты . . . 309
12.1. Знакомство с византийскими отказоустойчивыми алгоритмами консенсуса . . . 310
12.1.1. Проблема устойчивости и распределенные протоколы . . . 310
12.1.2. Децентрализация помогает решить проблему доверия . . . 312
12.1.3. Проблема масштаба. Общедоступные и устойчивые к цензуре сети . . . 313
12.2. Принцип работы системы Bitcoin . . . 315
12.2.1. Обработка пользовательских балансов и транзакций в системе Bitcoin . . . 316
12.2.2. Добыча BTC в эпоху цифрового золота . . . 318
12.2.3. Форки. Разрешение конфликтов при добыче криптовалюты . . . 321
12.2.4. Уменьшение размера блока с помощью деревьев Меркла . . . 324
12.3. Экскурсия по миру криптовалют . . . 326
12.3.1. Волатильность . . . 326
12.3.2. Время ожидания . . . 327
12.3.3. Размер блокчейна . . . 327
12.3.4. Конфиденциальность . . . 328
12.3.5. Энергоэффективность . . . 328
12.4. DiemBFT — византийский отказоустойчивый протокол консенсуса . . . 328
12.4.1. Безопасность и живость — два свойства протокола консенсуса BFT . . . 329
12.4.2. Раунд в протоколе DiemBFT . . . 329
12.4.3. Какое количество нечестных участников допускает протокол . . . 331
12.4.4. Правила голосования в DiemBFT . . . 331
12.4.5. Когда транзакции считаются завершенными . . . 332
12.4.6. Интуитивное понимание безопасности протокола DiemBFT . . . 333
Резюме . . . 336

Глава 13. Аппаратная криптография . . . 338
13.1. Модель злоумышленника в современной криптографии . . . 338
13.2. Недоверенные среды — аппаратное обеспечение спешит на помощь . . . 340
13.2.1. Криптография белого ящика — это плохая идея . . . 341
13.2.2. Они в вашем бумажнике: смарт-карты и защищенные элементы . . . 342
13.2.3. Излюбленные банками аппаратные модули безопасности . . . 345

13.2.4. Доверенные платформенные модули — полезная стандартизация защищенных элементов . . . 347
13.2.5. Конфиденциальные вычисления с помощью доверенной среды выполнения . . . 351
13.3. Какое решение подходит именно мне? . . . 352
13.4. Криптография, устойчивая к утечкам, или Как смягчить атаки по сторонним каналам в программном обеспечении . . . 354
13.4.1. Программирование операций, выполняемых за постоянное время . . . 357
13.4.2. Не используйте секрет! Маскировка и ослепление . . . 358
13.4.3. А как насчет атак по ошибкам вычислений? . . . 359
Резюме . . . 360

Глава 14. Постквантовая криптография . . . 362
14.1. Что такое квантовые компьютеры и почему они пугают криптографов . . . 363
14.1.1. Квантовая механика, изучение мельчайших частиц . . . 363
14.1.2. От создания квантовых компьютеров до квантового превосходства . . . 366
14.1.3. Влияние алгоритмов Гровера и Шора на криптографию . . . 367
14.1.4. Постквантовая криптография, защита от квантовых компьютеров . . . 369
14.2. Подписи на основе хеша: не нужно ничего, кроме хеш-функции . . . 369
14.2.1. Одноразовые подписи с подписями Лэмпорта . . . 370
14.2.2. Ключи меньшего размера с одноразовыми подписями Винтерница . . . 372
14.2.3. Многоразовые подписи с XMSS и SPHINCS+ . . . 374
14.3. Сокращение длины ключей и подписей с помощью криптографии на решетках . . . 378
14.3.1. Что такое решетка . . . 378
14.3.2. Обучение с ошибками — основа для криптографических систем? . . . 380
14.3.3. Kyber — обмен ключами на основе решеток . . . 381
14.3.4. Dilithium — схема цифровой подписи на основе решетки . . . 384
14.4. Стоит ли паниковать . . . 386
Резюме . . . 387

Глава 15. Криптография следующего поколения . . . 389
15.1. Чем больше народу, тем веселее: защищенные многосторонние вычисления . . . 390
15.1.1. Пересечение закрытых множеств . . . 391
15.1.2. MPC общего назначения . . . 392
15.1.3. Текущее состояние дел в сфере MPC . . . 395
15.2. Полностью гомоморфное шифрование и обещание зашифрованного облака . . . 395
15.2.1. Пример гомоморфного шифрования с помощью алгоритма RSA . . . 396
15.2.2. Различные типы гомоморфного шифрования . . . 397

15.2.3. Перешифрование — ключ к полностью гомоморфному шифрованию . . . 397
15.2.4. Схема полностью гомоморфного шифрования, основанная на задаче обучения с ошибками . . . 401
15.2.5. Сфера применения полностью гомоморфного шифрования . . . 402
15.3. Многоцелевые доказательства с нулевым разглашением . . . 403
15.3.1. Принцип работы схем zk-SNARK . . . 406
15.3.2. Гомоморфные обязательства для сокрытия частей доказательства . . . 407
15.3.3. Билинейные спаривания для улучшения гомоморфных обязательств . . . 407
15.3.4. Откуда берется лаконичность . . . 408
15.3.5. От программ к многочленам . . . 409
15.3.6. Программы предназначены для компьютеров, а нам нужны арифметические схемы . . . 410
15.3.7. От арифметической схемы к системе ограничений ранга 1 . . . 410
15.3.8. От системы ограничений ранга 1 к многочлену . . . 411
15.3.9. Для вычисления значения многочлена, скрытого в экспоненте, нужны двое . . . 412
Резюме . . . 414

Глава 16. Условия, в которых криптография может не сработать . . . 415
16.1. Поиск подходящего криптографического примитива или протокола — скучное занятие . . . 416
16.2. Как использовать криптографический примитив или протокол. Вежливые стандарты и формальная верификация . . . 417
16.3. Где искать хорошие библиотеки . . . 420
16.4. Злоупотребление криптографией. Разработчики — главные враги . . . 422
16.5. Вы делаете это неправильно: удобная безопасность . . . 423
16.6. Криптография — это не изолированный остров . . . 425
16.7. Ваша обязанность как практикующего криптографа состоит в том, чтобы не развертывать собственную криптографию . . . 425
Резюме . . . 427

Приложение. Ответы к упражнениям . . . 429