

УДК 004.382  
ББК 32.973-018  
О57

**Омассон Ж.-Ф.**

О57 О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2022. – 328 с.: ил.

**ISBN 978-5-97060-975-0**

В этом практическом руководстве по современному шифрованию анализируются фундаментальные математические идеи, лежащие в основе криптографии. Рассказывается о шифровании с аутентификацией, безопасной случайности, функциях хеширования, блочных шифрах и методах криптографии с открытым ключом, в частности RSA и криптографии на эллиптических кривых. Вы узнаете о том, как выбирать наилучший алгоритм или протокол, как избежать типичных ошибок безопасности и как задавать правильные вопросы поставщику. В заключительной части книги рассматриваются темы повышенной сложности, например TLS, а также обсуждается будущее криптографии в эпоху квантовых компьютеров.

В каждой главе приводятся примеры работы алгоритмов и материалы для дополнительного изучения.

Издание будет полезно как профессиональным разработчикам, так и тем, кто хочет разобраться в основах современной криптографии и успешно применять методы шифрования.

УДК 004.382  
ББК 32.973-018

Title of English-language original: Serious Cryptography: A Practical Introduction to Modern Encryption, ISBN 9781593278267, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2021 by DMK Press Publishing under license by No Starch Press Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-59327-826-7 (англ.)  
ISBN 978-5-97060-975-0 (рус.)

© Jean-Philippe Aumasson, 2018  
© Перевод, оформление,  
издание, ДМК Пресс, 2021

# 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

### **Глава 3. Криптографическая безопасность..... 65**

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

### **Глава 4. Блочные шифры..... 82**

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> .....	202
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> .....	221
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

## **Глава 14. Квантовая и постквантовая криптография .....**

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

## **Предметный указатель .....**