

Алгоритмы криптографии

Второе издание

Массимо Бертаччини

SPRINT
book

2026

Краткое содержание

Предисловие	12
Над книгой работали	16

Часть I

Краткая история и основы криптографии

Глава 1. Погружение в мир криптографии	20
--	----

Часть II

Классическая криптография

Глава 2. Алгоритмы симметричного шифрования.....	52
Глава 3. Алгоритмы асимметричного шифрования	89
Глава 4. Хеш-функции и цифровые подписи	114

Часть III

Новые криптографические алгоритмы и протоколы

Глава 5. Доказательство с нулевым разглашением.....	146
Глава 6. Новые изобретения в криптографии и логические атаки	174
Глава 7. Эллиптические кривые.....	227
Глава 8. Гомоморфное шифрование и система защищенного поиска.....	253

Часть IV

Квантовая криптография

Глава 9. Основы квантовой криптографии	284
Глава 10. Алгоритмы квантового поиска и квантовые вычисления	321

Оглавление

Предисловие	12
Для кого эта книга	13
Структура издания	13
Как получить максимальную пользу от книги	14
Условные обозначения	15
Над книгой работали	16
Об авторе	16
О научных редакторах	17
О бета-читателях	18
От издательства	18
О научном редакторе русскоязычного издания	18

Часть I

Краткая история и основы криптографии

Глава 1. Погружение в мир криптографии	20
Введение в криптографию	20
Двоичные числа, код ASCII и условные обозначения	25
Последняя теорема Ферма, простые числа и модульная арифметика	27
Краткая история и общий обзор криптографических алгоритмов	32
Розеттский камень	32
Шифр Цезаря	33
ROT13	36
Криптограммы Бейла	38
Шифр Вернама	44
Обеспечение безопасности и вычислений	47
Резюме	50

Часть II

Классическая криптография

Глава 2. Алгоритмы симметричного шифрования.....	52
Понятия и операции в булевой алгебре.....	52
Алгоритмы DES	57
Простой DES	58
DES	64
Triple DES.....	75
DESX.....	76
AES Rijndael	77
Описание AES	78
Атаки и уязвимости AES.....	82
Резюме.....	87
Глава 3. Алгоритмы асимметричного шифрования	89
Введение в асимметричное шифрование	89
Первопроходцы	90
Алгоритм Диффи — Хеллмана	92
Задача дискретного логарифма.....	94
Объяснение алгоритма Диффи — Хеллмана	96
Анализ алгоритма	97
Возможные атаки на алгоритм Диффи — Хеллмана и криптоанализ	98
RSA.....	100
Объяснение алгоритма RSA.....	101
Анализ RSA.....	103
Типичные атаки на алгоритм.....	104
Применение RSA для проверки международных соглашений.....	105
Нетипичные атаки	107
PGP.....	109
Схема Эль-Гамала.....	110
Резюме.....	113
Глава 4. Хеш-функции и цифровые подписи	114
Общее объяснение хеш-функций	115
Обзор основных хеш-алгоритмов.....	118
Операции и обозначения для реализации хеш-функций	119
Объяснение алгоритма SHA-1	124
Заметки и пример по SHA-1	128
Аутентификация и цифровые подписи	131
Цифровые подписи в RSA	133
Цифровые подписи в схеме Эль-Гамала	137
Слепые подписи	139
Резюме.....	143

Часть III

Новые криптографические алгоритмы и протоколы

Глава 5. Доказательство с нулевым разглашением.....	146
Основной сценарий ZKP — цифровая пещера	147
Неинтерактивные протоколы доказательства с нулевым разглашением	148
Демонстрация работы неинтерактивного протокола ZKP	151
Атака на неинтерактивный протокол RSA ZKP	152
Интерактивный протокол ZKP Шнора.....	154
Демонстрация интерактивного ZKP	155
Проверка разрушительной атаки на интерактивный ZKP	157
Однораундовый ZKP	158
Работа протокола с математической точки зрения.....	160
Введение в протоколы zk-SNARK — мистическая математика	162
Как работает протокол zk-SNARK.....	163
Демонстрация атаки на протокол zk-SNARK.....	165
ZK13 — протокол ZKP для аутентификации и обмена ключами.....	167
Объяснение ZK13	169
Демонстрация протокола ZK13	171
Возможные атаки на ZK13	172
Резюме.....	172
Глава 6. Новые изобретения в криптографии и логические атаки	174
История создания алгоритма MB09 и блокчейна.....	174
Введение в алгоритм MB09 и доказательство последней	
теоремы Ферма.....	179
Подробное объяснение алгоритма MB09.....	183
Открытые параметры	185
Введение в алгоритм MBXI.....	190
Нетрадиционные атаки и саморасшифровка в RSA	195
Новый протокол защиты RSA и асимметричные алгоритмы защиты	
от шпионажа.....	201
Цифровые подписи в MBXI	203
Создание прямой цифровой подписи в MBXI	205
Создание подписи с дополнением в MBXI.....	206
Демонстрация алгоритма создания цифровой подписи MBXI	
с точки зрения математики.....	207
Развитие MB09 и MBXI: введение в MBXX	210
Описание протокола MBXX.....	213
Легковесное шифрование.....	220
Алгоритм Cybpher	220
Шифрование в Cybpher.....	222
Тестирование производительности Cybpher	224
Резюме.....	225

Глава 7. Эллиптические кривые	227
Обзор эллиптических кривых.....	227
Операции, выполняемые на эллиптических кривых.....	228
Скалярное умножение	233
Реализация алгоритма Диффи — Хеллмана на эллиптических кривых	235
Эллиптическая кривая $secp256k1$ — цифровая подпись для «Биткойна»	240
Шаг 1. Генерирование ключей	242
Шаг 2. Создание цифровой подписи в $secp256k1$	243
Шаг 3. Проверка цифровой подписи	243
Числовой пример цифровой подписи на кривой $secp256k1$	244
Атаки на ECDSA и безопасность эллиптических кривых	248
Шаг 1. Восстановление случайного ключа $[k]$	248
Шаг 2. Восстановление закрытого ключа $[d]$	249
Взгляд на будущее эллиптической криптографии.....	251
Резюме	251
Глава 8. Гомоморфное шифрование и система защищенного поиска	253
Введение в CSE — гомоморфизм.....	253
Частичный гомоморфизм в RSA.....	256
Изучение гомоморфного шифрования и способы его применения	258
Математические и логические основы традиционных поисковых систем	260
Введение в деревья — теория графов	264
Код Хаффмана.....	266
Хеш-функции и булева алгебра.....	268
Объяснение CSE.....	270
Новаторство CSE.....	272
Анализ вычислительной эффективности CSE	275
Пример взлома методом грубой силы	277
Области применения CSE.....	279
Новый рубеж CSE и новый квантовый алгоритм передачи сообщений — QTM	281
Резюме	282

Часть IV

Квантовая криптография

Глава 9. Основы квантовой криптографии	284
Введение в Q-механику и Q-криптографию.....	284
Эксперимент, изменивший историю кванта	285
Мысленный эксперимент для понимания элементов Q-механики	286
Этап 1. Суперпозиция	287
Этап 2. Принцип неопределенности	289
Этап 3. Спин и запутанность	290

Происхождение Q-криптографии: квантовые деньги	294
QKD: BB84	297
Шаг 1. Инициализация квантового канала	299
Шаг 2. Передача фотонов	299
Шаг 3. Определение общего ключа	300
Атаки и технические вопросы	302
Квантовые вычисления	306
Алгоритм Шора	309
Гипотеза и тезис	310
Шаг 1. Инициализация кубитов	310
Шаг 2. Выбор случайного числа (a)	311
Шаг 3. Квантовое измерение	312
Шаг 4. Поиск подходящего варианта (r)	313
Шаг 5. Факторизация (n)	317
Заметки об алгоритме Шора	318
Пост-Q-криптография	318
Резюме	320
Глава 10. Алгоритмы квантового поиска и квантовые вычисления	321
Обзор алгоритма Гровера	321
Элементы квантового программирования — квантовая информация и схемы	324
Классическая информация	324
Квантовая информация, вентили и схемы	327
Глубокое погружение в алгоритм Гровера	333
Псевдокод для выполнения алгоритма Гровера	336
Задача поиска с единственным решением и вероятность усиления амплитуды	342
Резюме	349