

Рябко Б. Я.
Фионов А. Н.

ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

Горячая линия-Телеком



2 издание

Б. Я. Рябко, А. Н. Фионов

**ОСНОВЫ СОВРЕМЕННОЙ
КРИПТОГРАФИИ И
СТЕГАНОГРАФИИ**

2 издание

Москва
Горячая линия - Телеком
2013

УДК 621.391
ББК 32.801.4
Р98

Рябко Б. Я., Фионов А. Н.

Р98 Основы современной криптографии и стеганографии. – 2-е изд. – М.: Горячая линия – Телеком, 2013. – 232 с.: ил.
ISBN 978-5-9912-0350-0.

В монографии изложены основные подходы и методы современной криптографии и стеганографии для решения задач, возникающих при обработке, хранении и передаче информации. Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блочные и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо невскрываемых криптосистем и криптографии на эллиптических кривых. Рассмотрены вопросы, связанные с использованием случайных и псевдослучайных чисел в системах защиты информации. Приведено описание основных идей и методов современной стеганографии. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов. Многие из приведенных в книге результатов исследований, полученных авторами в последние годы, признаны специалистами в России и за рубежом.

Для исследователей и специалистов, работающих в области защиты информации, будет полезна для аспирантов и студентов.

ББК 32.801.4

Адрес издательства в Интернет www.techbook.ru

Научное издание

Рябко Борис Яковлевич
Фионов Андрей Николаевич

Основы современной криптографии и стеганографии

Монография

2-е издание

Подписано к печати 15.06.2013. Формат 60×88 1/16. Усл. печ. л. 14,5. Изд. № 130350.
Тираж 300 экз. (1-й завод 100 экз.)

ISBN 978-5-9912-0350-0

© Б. Я. Рябко, А. Н. Фионов, 2011, 2013

© Издательство «Горячая линия–Телеком», 2013

ОГЛАВЛЕНИЕ

Предисловие	3
1. Введение	5
2. Криптосистемы с открытым ключом	12
2.1. Предыстория и основные идеи	12
2.2. Первая система с открытым ключом — система Диффи–Хеллмана	18
2.3. Элементы теории чисел	21
2.4. Шифр Шамира	28
2.5. Шифр Эль-Гамала	31
2.6. Односторонняя функция с «лазейкой» и шифр RSA	34
3. Методы взлома шифров, основанных на дискретном логарифмировании	38
3.1. Постановка задачи	38
3.2. Метод «шаг младенца, шаг великана»	40
3.3. Алгоритм исчисления порядка	42
4. Электронная, или цифровая подпись	48
4.1. Электронная подпись RSA	48
4.2. Электронная подпись на базе шифра Эль-Гамала	51
4.3. Стандарты на электронную (цифровую) подпись	54
5. Криптографические протоколы	59
5.1. Ментальный покер	59
5.2. Доказательства с нулевым знанием	64
Задача о раскраске графа	65
Задача о нахождении гамильтонова цикла в графе	68
5.3. Электронные деньги	76
5.4. Взаимная идентификация с установлением ключа	82

6. Криптосистемы на эллиптических кривых	89
6.1. Введение	89
6.2. Математические основы	90
6.3. Выбор параметров кривой	98
6.4. Построение криптосистем	100
Шифр Эль-Гамала на эллиптической кривой	101
Цифровая подпись по ГОСТ Р34.10-2001	102
6.5. Эффективная реализация операций	103
6.6. Определение количества точек на кривой	109
6.7. Использование стандартных кривых	118
7. Теоретическая стойкость криптосистем	121
7.1. Введение	121
7.2. Теория систем с совершенной секретностью	122
7.3. Шифр Вернама	124
7.4. Элементы теории информации	125
7.5. Расстояние единственности шифра с секретным ключом	132
7.6. Идеальные криптосистемы	138
8. Современные шифры с секретным ключом	145
8.1. Введение	145
8.2. Блочные шифры	148
Шифр ГОСТ 28147-89	150
Шифр RC6	153
Шифр Rijndael (AES)	156
8.3. Основные режимы функционирования блочных шиф- ров	166
Режим ECB	166
Режим CBC	167
8.4. Поточковые шифры	168
Режим OFB блочного шифра	170
Режим CTR блочного шифра	171
Алгоритм RC4	172
8.5. Криптографические хеш-функции	174
9. Случайные числа в криптографии	177
9.1. Введение	177
9.2. Задачи, возникающие при использовании физических генераторов случайных чисел	179

9.3. Генераторы псевдослучайных чисел	181
9.4. Тесты для проверки генераторов случайных и псевдо- случайных чисел	184
9.5. Статистическая атака на блочные шифры	189
10. Стеганография и стегоанализ	202
10.1. Назначение и применение стеганографии в современ- ных информационных технологиях	202
10.2. Основные методы встраивания скрытых данных . . .	208
10.3. Стегоанализ на основе сжатия данных	213
10.4. Асимптотически оптимальные совершенные стеганогра- фические системы	215
Список литературы	225