

**Лось, А. Б.**

Криптографические методы защиты информации : Учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — М. : Издательство Юрайт, 2016. — 473 с. — Серия : Бакалавр. Академический курс.

# ОГЛАВЛЕНИЕ

<b>Предисловие</b>	<b>9</b>
<b>Глава 1. Исторический очерк</b>	<b>11</b>
<b>Глава 2. Основные понятия и задачи криптографии</b>	<b>42</b>
2.1. Задачи криптографии и средства их решения	42
2.1.1. Конфиденциальность	43
2.1.2. Целостность	45
2.1.3. Аутентификация	46
2.2. Формальные модели шифров	47
2.2.1. Модель шифра простой замены	49
2.2.2. Модель шифра перестановки	51
2.2.3. Модель шифра маршрутной перестановки	52
2.2.4. Модель поточного шифра	54
2.2.5. Модель композиции шифров	55
2.3. Модели открытых текстов	56
2.3.1. Простейшая вероятностная модель	57
2.3.2. Модель на основе независимых /с-грамм	59
2.3.3. Марковская модель	59
2.3.4. Критерии на открытый текст	60
2.4. Оценки числа смысловых открытых текстов	62
2.4.1. Комбинаторный метод	62
2.4.2. Теоретико-информационный метод	62
2.4.3. Экспериментальные методы оценки энтропии языка	64
Задачи и упражнения	65
Дополнительная литература к 2-й главе	65
<b>Глава 3. Шифры гаммирования</b>	<b>66</b>
3.1. Определение операции гаммирования	66
3.2. Методы вскрытия шифра гаммирования	68
3.2.1. Использование неравновероятной гаммы	68
3.2.2. Повторное использование гаммы	69
3.2.3. Книжная гамма	71
3.2.4. Шифрование гаммой короткого периода	72
Задачи и упражнения	75
Дополнительная литература к 3-й главе	76

<b>Глава 4. Оценка качества криптографических преобразований</b>	<b>77</b>
4.1. Понятие стойкости шифра	77
4.1.1. Практическая стойкость	77
4.1.2. Другие подходы к оценке практической стойкости	78
4.2. Теоретическая стойкость по Шеннону	80
4.3. Основные задачи и методы криптоанализа	83
4.3.1. Метод полного перебора ключей	85
4.3.2. Эквивалентные ключи	87
4.3.3. Расстояние единственности	90
4.3.4. Имитостойкость	92
Задачи и упражнения	95
Дополнительная литература к 4-й главе	96
<b>Глава 5. Свойства криптографических преобразований</b>	<b>97</b>
5.1. Булевы функции и их характеристики	97
5.1.1. Многочлен Жегалкина	97
5.1.2. Вес булевой функции	98
5.1.3. Разложение в ряд Фурье	99
5.1.4. Преобразование Уолша-Адамара	99
5.1.5. Статистическая структура	100
5.1.6. Расстояние между булевыми функциями	100
5.2. Статистические аналоги	101
5.3. Бент-функции	104
5.4. Корреляционно-иммунные функции	106
5.5. Строгий лавинный критерий и критерий распространения	109
5.6. Группа инерции	110
5.7. Сильная равномерность булевых функций	114
5.8. Семейство координатных булевых функций	118
5.9. Ортогональные системы выходных функций фильтрующего генератора	120
5.10. Перемешивающие свойства отображений	126
5.11. Функции $A$ -значной логики	127
5.12. Узлы модульного суммирования	128
5.12.1. Суммирование по модулю $t = 4$	132
5.12.2. Суммирование в группе $G = \mathbb{Z}_2 \times \mathbb{Z}_2$	132
5.12.3. Суммирование в циклической группе $G = \mathbb{Z}_m$	133
5.12.4. Суммирование в группе $G = G \setminus x$	136
5.12.5. Устойчивые законы распределения	136
5.13. MDS-матрицы над полем $F^q$	138
5.13.1. Основные понятия и определения	138
5.13.2. Бирегулярные матрицы	141
5.13.3. Примеры MDS-матриц над полем $F_{2^s}$	144

5.13.4. Примеры MDS-матриц $A^{\chi_8}$ над полем $F_2^s$ . . .	146
Дополнительная литература к 5-й главе. . . . .	148

<b>Глава 6. Поточные шифры и генерация псевдослучайных последовательностей</b>	<b>150</b>
6.1. Линейный регистр сдвига . . . . .	152
6.1.1. Линейные рекуррентные последовательности . . . . .	153
6.1.2. Оценка длины периода . . . . .	155
6.1.3. Минимальный многочлен последовательности . . . . .	158
6.1.4. Линейная рекуррентная последовательность максимального периода . . . . .	162
6.1.5. Семейства линейных рекуррентных последовательностей . . . . .	164
6.1.6. Представление элементов линейной рекуррентной последовательности через функцию след . . . . .	166
6.2. Фильтрующий и комбинирующий генераторы . . . . .	169
6.2.1. Фильтрующие генераторы . . . . .	170
6.2.2. Комбинирующие генераторы . . . . .	172
6.2.3. Аналитические методы анализа фильтрующего генератора . . . . .	174
6.2.4. Статистические методы анализа комбинирующего генератора . . . . .	179
6.3. Статистические свойства фильтрующей схемы . . . . .	182
6.3.1. Статистическая неотличимость булевых функций . . . . .	182
6.3.2. Выборка из выходной последовательности . . . . .	185
6.3.3. Выборка с минимальным зацеплением . . . . .	188
6.3.4. Оценка мощности множеств $M(A_1, A_2)$ . . . . .	189
6.3.5. Оценка мощности множеств $M(0, A_2, A_3)$ . . . . .	190
6.3.6. Классификация функций от $n^3$ переменных . . . . .	190
6.4. Другие методы построения ГСП . . . . .	192
6.4.1. Генераторы с неравномерным движением . . . . .	192
6.4.2. Регистры сдвига с нелинейной обратной связью . . . . .	194
6.4.3. Аддитивный генератор . . . . .	197
6.4.4. Линейный конгруэнтный генератор . . . . .	197
6.4.5. Генератор BBS . . . . .	198
6.4.6. Генератор RSA . . . . .	199
6.4.7. Генератор Макларена-Марсальи . . . . .	199
6.5. Примеры алгоритмов поточного шифрования . . . . .	200
6.5.1. Алгоритм A5 . . . . .	200
6.5.2. Алгоритм RC4 . . . . .	201
6.5.3. Алгоритм Grain-128 . . . . .	204
Задачи и упражнения . . . . .	207
Дополнительная литература к 6-й главе. . . . .	208

<b>Глава 7. Блочные шифры</b>	<b>209</b>
7.1. История вопроса . . . . .	209
7.2. Формальное определение блочного шифра . . . . .	211
7.3. Структура блочного алгоритма шифрования . . . . .	213
7.4. Сеть Фейстеля . . . . .	215
7.4.1. Алгоритм DES . . . . .	216
7.4.2. Алгоритм «Магма» (ГОСТ 28147-89) . . . . .	219
7.4.3. Обобщенная сеть Фейстеля: алгоритм RC6 . . . . .	222
7.5. SP-сеть . . . . .	227
7.5.1. Алгоритм AES . . . . .	228
7.5.2. Алгоритм «Кузнечик» . . . . .	239
7.6. Режимы использования блочных шифров . . . . .	246
7.6.1. Режим простой замены . . . . .	249
7.6.2. Режим гаммирования . . . . .	251
7.6.3. Режим гаммирования с обратной связью по шифртексту . . . . .	255
7.6.4. Режим счетчика . . . . .	256
7.6.5. Режим простой замены с зацеплением . . . . .	258
7.6.6. Режим шифрования блочных устройств . . . . .	263
Задачи и упражнения . . . . .	269
Дополнительная литература к 7-й главе . . . . .	269
<b>Глава 8. Функции хэширования</b>	<b>270</b>
8.1. Бесключевые функции хэширования . . . . .	271
8.1.1. Методы построения функций хэширования . . . . .	272
8.1.2. Функция ГОСТ Р 34.11-94 . . . . .	276
8.1.3. Функция «Стрибог» (ГОСТ Р 34.11-2012) . . . . .	279
8.1.4. Некоторые вопросы анализа функций хэширования . . . . .	283
8.2. Ключевые функции хэширования . . . . .	284
8.2.1. Функция HMAC . . . . .	287
8.2.2. Функции, использующие алгоритмы блочного шифрования . . . . .	289
8.2.3. Универсальные функции хэширования . . . . .	293
8.2.4. Режимы шифрования с возможностью аутентификации . . . . .	296
Задачи и упражнения . . . . .	300
Дополнительная литература к 8-й главе . . . . .	301
<b>Глава 9. Элементы теории чисел</b>	<b>302</b>
9.1. Алгоритм Эвклида . . . . .	303
9.2. Сравнения первой степени . . . . .	305
9.3. Функция Эйлера и первообразные корни . . . . .	309
9.4. Эллиптические кривые . . . . .	312
9.4.1. Основные определения . . . . .	313

9.4.2. Групповой закон . . . . .	315
9.4.3. Эллиптические кривые над кольцами . . . . .	318
Задачи и упражнения . . . . .	320
Дополнительная литература к 9-й главе . . . . .	320
<b>Глава 10. Асимметричное шифрование</b>	<b>321</b>
10.1. Схема шифрования RSA . . . . .	323
10.1.1. Схема шифрования RSA: теория . . . . .	325
10.1.2. Схема шифрования RSA: практика . . . . .	341
10.2. Схема шифрования Рабина-Вильямса . . . . .	347
10.3. Схема шифрования Эль-Гамала . . . . .	349
10.4. Схема шифрования Окамото-Учиямы . . . . .	351
10.5. Схема шифрования Мейера-Мюллера . . . . .	353
10.6. Гибридная схема шифрования . . . . .	355
Задачи и упражнения . . . . .	358
Дополнительная литература к 10-й главе . . . . .	359
<b>Глава 11. Электронная подпись</b>	<b>360</b>
11.1. О группе точек эллиптической кривой . . . . .	363
11.2. Схема Эль-Гамала . . . . .	364
11.2.1. Стандарт ГОСТ Р 34.10-2012 . . . . .	365
11.2.2. Стандарт ECDSA . . . . .	368
11.3. Схема Шнорра . . . . .	371
11.4. Схема Ньюберг-Рюппеля . . . . .	372
11.5. Схема KCDSA . . . . .	373
Задачи и упражнения . . . . .	374
Дополнительная литература к 11-й главе . . . . .	374
<b>Глава 12. Управление ключами</b>	<b>375</b>
12.1. Характеристики ключевой системы . . . . .	376
12.1.1. Жизненный цикл ключей . . . . .	376
12.1.2. Роль доверенной третьей стороны . . . . .	377
12.1.3. Строение ключевого множества . . . . .	378
12.1.4. Производные ключи . . . . .	379
12.2. Разделение секрета . . . . .	381
12.3. Стойкость к компрометации заданного числа абонен- тов . . . . .	383
12.4. Протоколы выработки общего ключа . . . . .	386
12.4.1. Базовый протокол Диффи-Хеллмана . . . . .	387
12.4.2. Протокол со взаимной аутентификацией . . . . .	388
12.4.3. Семейство протоколов МТИ . . . . .	389
12.4.4. Выработка ключа для конференц-связи . . . . .	396
12.5. Протоколы передачи ключей . . . . .	397
12.5.1. Двусторонние протоколы . . . . .	397
12.5.2. Трехсторонние протоколы . . . . .	397

12.5.3. Передача ключей с помощью асимметричного шифрования . . . . .	398
12.5.4. Транспортный протокол Шамира . . . . .	399
Задачи и упражнения . . . . .	400
Дополнительная литература к 12-й главе . . . . .	401
<b>Глава 13. Некоторые методы решения сложных задач теории чисел</b>	<b>402</b>
13.1. Построение простых чисел . . . . .	402
13.1.1. Вероятностные тесты проверки простоты . . . . .	404
13.1.2. « $N - 1$ » методы доказательства простоты . . . . .	406
13.1.3. Рекурсивный алгоритм построения простых чисел . . . . .	410
13.1.4. Алгоритм построения сильно простого числа . . . . .	412
13.2. Методы разложения чисел на множители . . . . .	415
13.2.1. Метод пробного деления . . . . .	415
13.2.2. Метод Ферма . . . . .	416
13.2.3. « $p - 1$ » метод Полларда . . . . .	417
13.2.4. Метод Ленстры . . . . .	419
13.2.5. Метод Крайчика . . . . .	421
13.2.6. Метод квадратичного решета и его вариации . . . . .	423
13.3. Дискретное логарифмирование . . . . .	429
13.3.1. Метод согласования . . . . .	431
13.3.2. Метод Полига-Хеллмана . . . . .	433
13.3.3. Метод Нечаева . . . . .	435
13.3.4. Метод Полларда-Флойда . . . . .	437
13.3.5. Метод Госпера . . . . .	439
Задачи и упражнения . . . . .	441
Дополнительная литература к 13-й главе . . . . .	442
<b>Глава 14. Нормативная база в области криптографической защиты информации</b>	<b>443</b>
14.1. Федеральные законы . . . . .	443
14.2. Ведомственные акты . . . . .	447
14.2.1. Положение ПКЗ-2005 . . . . .	448
14.2.2. Положение о лицензировании . . . . .	450
14.2.3. Требования к средствам электронной подписи . . . . .	456
14.2.4. Требования к средствам удостоверяющего центра . . . . .	458
14.3. Национальные стандарты Российской Федерации . . . . .	462
Задачи и упражнения . . . . .	465
<b>Указатель обозначений</b>	<b>466</b>
<b>Предметный указатель</b>	<b>468</b>