

А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УЧЕБНИК ДЛЯ АКАДЕМИЧЕСКОГО БАКАЛАВРИАТА

2-е издание, исправленное

*Рекомендовано Учебно-методическим отделом высшего образования
в качестве учебника для студентов высших учебных заведений,
обучающихся по инженерно-техническим направлениям и специальностям*

**Книга доступна в электронной библиотеке biblio-online.ru,
а также в мобильном приложении «Юрайт.Библиотека»**

Москва ■ Юрайт ■ 2019

УДК 004.056(075.8)
ББК 32.811.4я73
Л79

Авторы:

Лось Алексей Борисович — кандидат технических наук, доцент, заведующий кафедрой компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Нестеренко Алексей Юрьевич — кандидат физико-математических наук, доцент кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»;

Рожков Михаил Иванович — доктор технических наук, старший научный сотрудник, профессор кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики».

Рецензенты:

Хаматов В. М. — доктор юридических наук, профессор, почетный работник высшего профессионального образования РФ, заведующий кафедрой уголовно-процессуального права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА);

Попов В. Л. — доктор физико-математических наук, профессор Математического института имени В. А. Стеклова.

Лось, А. Б.

Л79 Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2019. — 473 с. — (Серия : Бакалавр. Академический курс).

ISBN 978-5-534-10673-2

В учебнике «Криптографические методы защиты информации» изложен курс алгоритмической теории чисел и ее приложений к вопросам защиты информации. Основное внимание уделено строгому математическому обоснованию, эффективной реализации и анализу трудоемкости алгоритмов, используемых в криптографических приложениях. Приведено описание современных криптографических схем и протоколов, использующих изложенные теоретические сведения.

В отличие от существующих пособий по данной тематике учебник содержит в себе изложение, построенное по принципу «от простого к сложному», что позволит освоить рассматриваемый материал без существенного использования дополнительной литературы.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Для студентов, учащихся по специальности «Компьютерная безопасность», магистрантов, обучающихся по специальности «Математические методы защиты информации», а также аспирантов и научных работников.

УДК 004.056(075.8)
ББК 32.811.4я73



Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Правовую поддержку издательства обеспечивает юридическая компания «Дельфи».

ISBN 978-5-534-10673-2

© Лось А. Б., Нестеренко А. Ю., Рожков М. И., 2012
© Лось А. Б., Нестеренко А. Ю., Рожков М. И., 2016,
с изменениями
© ООО «Издательство Юрайт», 2019

Оглавление

Предисловие	9
Указатель обозначений.....	11
Глава 1. Исторический очерк.....	13
Дополнительная литература к главе 1	35
Глава 2. Основные понятия и задачи криптографии	37
2.1. Задачи криптографии и средства их решения	37
2.1.1. Конфиденциальность	38
2.1.2. Целостность.....	39
2.1.3. Аутентификация.....	40
2.2. Формальные модели шифров.....	41
2.2.1. Модель шифра простой замены.....	43
2.2.2. Модель шифра перестановки	44
2.2.3. Модель шифра маршрутной перестановки.....	46
2.2.4. Модель поточного шифра	47
2.2.5. Модель композиции шифров.....	49
2.3. Модели открытых текстов.....	49
2.3.1. Простейшая вероятностная модель	50
2.3.2. Модель на основе независимых k -грамм	52
2.3.3. Марковская модель	53
2.3.4. Критерии на открытый текст	53
2.4. Оценки числа смысловых открытых текстов	55
2.4.1. Комбинаторный метод.....	55
2.4.2. Теоретико-информационный метод.....	55
2.4.3. Экспериментальные методы оценки энтропии языка.....	57
Задачи и упражнения.....	58
Дополнительная литература к главе 2	58
Глава 3. Шифры гаммирования	59
3.1. Определение операции гаммирования	59
3.2. Методы вскрытия шифра гаммирования	61
3.2.1. Использование неравновероятной гаммы.....	61
3.2.2. Повторное использование гаммы	62
3.2.3. Книжная гамма	64
3.2.4. Шифрование гаммой короткого периода	64
Задачи и упражнения.....	67
Дополнительная литература к главе 3	67

Глава 4. Оценка качества криптографических преобразований ...	68
4.1. Понятие стойкости шифра	68
4.1.1. Практическая стойкость	68
4.1.2. Другие подходы к оценке практической стойкости	69
4.2. Теоретическая стойкость по Шеннону	71
4.3. Основные задачи и методы криптоанализа	74
4.3.1. Метод полного перебора ключей	75
4.3.2. Эквивалентные ключи	77
4.3.3. Расстояние единственности	79
4.3.4. Имитостойкость	81
<i>Задачи и упражнения</i>	84
<i>Дополнительная литература к главе 4</i>	84
Глава 5. Свойства криптографических преобразований.....	86
5.1. Булевы функции и их характеристики	86
5.1.1. Многочлен Жегалкина	86
5.1.2. Вес булевой функции	87
5.1.3. Разложение в ряд Фурье	88
5.1.4. Преобразование Уолша — Адамара	88
5.1.5. Статистическая структура	88
5.1.6. Расстояние между булевыми функциями	89
5.2. Статистические аналоги	89
5.3. Бент-функции	92
5.4. Корреляционно-иммунные функции	94
5.5. Строгий лавинный критерий и критерий распространения	97
5.6. Группа инерции	98
<i>Задачи и упражнения к параграфу 5.6</i>	101
5.7. Сильная равномерность булевых функций	101
<i>Задачи и упражнения к параграфу 5.7</i>	104
5.8. Семейство координатных булевых функций	105
5.9. Ортогональные системы выходных функций фильтрующего генератора	107
<i>Задачи и упражнения к параграфу 5.9</i>	112
5.10. Перемешивающие свойства отображений	112
5.11. Функции k -значной логики	113
5.12. Узлы модульного суммирования	114
5.12.1. Суммирование по модулю $m = 4$	118
5.12.2. Суммирование в группе $G = \mathbb{Z}_2 \times \mathbb{Z}_2$	118
5.12.3. Суммирование в циклической группе $G = \mathbb{Z}_m$	119
5.12.4. Суммирование в группе $G = G_1 \times G_2$	122
5.12.5. Устойчивые законы распределения	122
<i>Задачи и упражнения к параграфу 5.12</i>	123
5.13. MDS-матрицы над полем $\mathbb{F}_q$	124
5.13.1. Основные понятия и определения	124
5.13.2. Бирегулярные матрицы	126
5.13.3. Примеры MDS-матриц $A_{4 \times 4}$ над полем $\mathbb{F}_{2^8}$	129

5.13.4. Примеры MDS-матриц $A_{8 \times 8}$ над полем $\mathbb{F}_{2^8}$	131
<i>Дополнительная литература к главе 5</i>	133
Глава 6. Поточные шифры и генерация псевдослучайных последовательностей	135
6.1. Линейный регистр сдвига	137
6.1.1. Линейные рекуррентные последовательности	137
6.1.2. Оценка длины периода	140
6.1.3. Минимальный многочлен последовательности	143
6.1.4. Линейная рекуррентная последовательность максимального периода	146
6.1.5. Семейства линейных рекуррентных последовательностей	148
6.1.6. Представление элементов линейной рекуррентной последовательности через функцию след	150
<i>Задачи и упражнения к параграфу 6.1</i>	152
6.2. Фильтрующий и комбинирующий генераторы	153
6.2.1. Фильтрующие генераторы	153
6.2.2. Комбинирующие генераторы	155
6.2.3. Аналитические методы анализа фильтрующего генератора	157
6.2.4. Статистические методы анализа комбинирующего генератора	162
6.3. Статистические свойства фильтрующей схемы	164
6.3.1. Статистическая неотличимость булевых функций	164
6.3.2. Выборка из выходной последовательности	167
6.3.3. Выборка с минимальным зацеплением	170
6.3.4. Оценка мощности множеств $M(\lambda_1, \lambda_2)$	172
6.3.5. Оценка мощности множеств $M(0, \lambda_2, \lambda_3)$	172
6.3.6. Классификация функций от $n \leq 3$ переменных	172
6.4. Другие методы построения ГСП	174
6.4.1. Генераторы с неравномерным движением	174
6.4.2. Регистры сдвига с нелинейной обратной связью	175
6.4.3. Аддитивный генератор	178
6.4.4. Линейный конгруэнтный генератор	178
6.4.5. Генератор BBS	179
6.4.6. Генератор RSA	180
6.4.7. Генератор Макларена — Марсальи	180
6.5. Примеры алгоритмов поточного шифрования	181
6.5.1. Алгоритм A5	181
6.5.2. Алгоритм RC4	182
6.5.3. Алгоритм Grain-128	184
<i>Задачи и упражнения</i>	187
<i>Дополнительные задачи для самостоятельных исследований функций от $n \geq 4$ переменных</i>	187
<i>Дополнительная литература к главе 6</i>	188
Глава 7. Блочные шифры	189
7.1. История вопроса	189

7.2. Формальное определение блочного шифра	191
7.3. Структура блочного алгоритма шифрования.....	192
7.4. Сеть Фейстеля	194
7.4.1. Алгоритм DES	195
7.4.2. Алгоритм «Магма» (ГОСТ 28147—89).....	198
7.4.3. Обобщенная сеть Фейстеля: алгоритм RC6.....	200
7.5. SP-сеть.....	204
7.5.1. Алгоритм AES	206
7.5.2. Алгоритм «Кузнечик».....	215
7.6. Режимы использования блочных шифров.....	222
7.6.1. Режим простой замены	224
7.6.2. Режим гаммирования	226
7.6.3. Режим гаммирования с обратной связью по шифртексту.....	229
7.6.4. Режим счетчика.....	231
7.6.5. Режим простой замены с зацеплением	233
7.6.6. Режим шифрования блочных устройств	237
Задачи и упражнения	242
Дополнительная литература к главе 7	243
Глава 8. Функции хэширования	244
8.1. Бесключевые функции хэширования	245
8.1.1. Методы построения функций хэширования	246
8.1.2. Функция ГОСТ Р 34.11—94.....	249
8.1.3. Функция «Стрибог» (ГОСТ Р 34.11—2012).....	252
8.1.4. Некоторые вопросы анализа функций хэширования.....	255
8.2. Ключевые функции хэширования	257
8.2.1. Функция HMAC.....	259
8.2.2. Функции, использующие алгоритмы блочного шифрования ...	261
8.2.3. Универсальные функции хэширования	264
8.2.4. Режимы шифрования с возможностью аутентификации	267
Задачи и упражнения	270
Дополнительная литература к главе 8	270
Глава 9. Элементы теории чисел	272
9.1. Алгоритм Евклида	273
9.2. Сравнения первой степени	275
9.3. Функция Эйлера и первообразные корни	278
9.4. Эллиптические кривые	282
9.4.1. Основные определения	282
9.4.2. Групповой закон	285
9.4.3. Эллиптические кривые над кольцами	287
Задачи и упражнения	289
Дополнительная литература к главе 9	289
Глава 10. Асимметричное шифрование	290
10.1. Схема шифрования RSA	292
10.1.1. Схема шифрования RSA: теория.....	293

10.2. Схема шифрования Рабина — Вильямса	314
10.3. Схема шифрования Эль-Гамала	316
10.4. Схема шифрования Окамото — Учиямы	317
10.5. Схема шифрования Мейера — Мюллера	319
10.6. Гибридная схема шифрования	321
Задачи и упражнения	324
Дополнительная литература к главе 10	324
Глава 11. Электронная подпись	325
11.1. О группе точек эллиптической кривой	327
11.2. Схема Эль-Гамала	328
11.2.1. Стандарт ГОСТ Р 34.10—2012	330
11.2.2. Стандарт ECDSA	332
11.3. Схема Шнорра	334
11.4. Схема Нюберг — Рюппеля	335
11.5. Схема KCDSA	336
Задачи и упражнения	337
Дополнительная литература к главе 11	338
Глава 12. Управление ключами	339
12.1. Характеристики ключевой системы	340
12.1.1. Жизненный цикл ключей	340
12.1.2. Роль доверенной третьей стороны	341
12.1.3. Строение ключевого множества	341
12.1.4. Производные ключи	342
12.2. Разделение секрета	344
12.3. Стойкость к компрометации заданного числа абонентов	346
12.4. Протоколы выработки общего ключа	349
12.4.1. Базовый протокол Диффи — Хеллмана	350
12.4.2. Протокол со взаимной аутентификацией	350
12.4.3. Семейство протоколов МТИ	351
12.4.4. Выработка ключа для конференц-связи	357
12.5. Протоколы передачи ключей	358
12.5.1. Двусторонние протоколы	358
12.5.2. Трехсторонние протоколы	359
12.5.3. Передача ключей с помощью асимметричного шифрования	359
12.5.4. Транспортный протокол Шамира	360
Задачи и упражнения	361
Дополнительная литература к главе 12	362
Глава 13. Некоторые методы решения сложных задач теории чисел	363
13.1. Построение простых чисел	363
13.1.1. Вероятностные тесты проверки простоты	365
13.1.2. «N – 1» методы доказательства простоты	367
13.1.3. Рекурсивный алгоритм построения простых чисел	370

13.1.4. Алгоритм построения сильно простого числа	372
13.2. Методы разложения чисел на множители	375
13.2.1. Метод пробного деления	375
13.2.2. Метод Ферма	376
13.2.3. « $P - 1$ » метод Полларда	377
13.2.4. Метод Ленстры	379
13.2.5. Метод Крайчика	380
13.2.6. Метод квадратичного решета и его вариации	382
13.3. Дискретное логарифмирование	388
13.3.1. Метод согласования	389
13.3.2. Метод Полига — Хеллмана	391
13.3.3. Метод Нечаева	393
13.3.4. Метод Полларда — Флойда	395
13.3.5. Метод Госпера	397
Задачи и упражнения	399
Дополнительная литература к главе 13	399
Глава 14. Нормативная база в области криптографической защиты информации	400
14.1. Федеральные законы	400
14.2. Ведомственные акты	404
14.2.1. Положение ПКЗ—2005	404
14.2.2. Положение о лицензировании	406
14.2.3. Требования к средствам электронной подписи	410
14.2.4. Требования к средствам удостоверяющего центра	412
14.3. Национальные стандарты Российской Федерации	415
Задачи и упражнения	417
Алфавитный указатель	418
Новинки по дисциплине	424