

ВЫСШЕЕ ОБРАЗОВАНИЕ

В. М. Фомичёв, Д. А. Мельников

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Часть 2. Системные и прикладные аспекты

Под редакцией В. М. Фомичёва

УЧЕБНИК



СООТВЕТСТВУЕТ
ПРОГРАММАМ
ВЕДУЩИХ НАУЧНО-
ОБРАЗОВАТЕЛЬНЫХ
ШКОЛ

УМО ВО рекомендует

Юрайт
издательство

Оглавление

Список основных обозначений.....	9
----------------------------------	---

Раздел I КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

Глава 12. Системные и исторические аспекты криптологии.....	13
12.1. Криптология — часть теории защиты информации.....	13
12.2. Разделы и научные источники криптологии.....	15
12.3. Основные термины и современные задачи криптографии и криптоанализа	16
12.4. Классификация криптографических систем и методов анализа.....	18
12.5. Об истории развития шифров	21
12.5.1. Развитие шифров домашней эры	21
12.5.2. Исторические очерки о развитии шифровальной службы в России.....	27
12.5.3. От ручных шифров — к шифрмашинам и компьютерным программам.....	28
<i>Контрольные вопросы и задания.....</i>	<i>32</i>
Глава 13. Математические модели источников открытых сообщений и шифров	33
13.1. Детерминированные модели источников открытых сообщений	33
13.2. Вероятностные модели источников открытых сообщений.....	34
13.2.1. Стационарный источник независимых символов алфавита.....	35
13.2.2. Стационарный источник независимых биграмм	36
13.2.3. Стационарный источник марковски зависимых букв	37
13.2.4. Усложнение стационарных моделей	37
13.2.5. Нестационарные источники сообщений.....	38
13.3. Построение и использование моделей источников открытых сообщений	38
13.4. Детерминированные модели криптографических функций.....	39
13.5. Автоматные модели симметричных криптосистем.....	40
13.6. Вероятностные модели криптосистем	41
13.7. Совершенно стойкие шифры	42
<i>Контрольные вопросы и задания.....</i>	<i>44</i>
Глава 14. Поточные шифры	46
14.1. Различия между поточными и блочными шифрами	46
14.2. Синхронные и самосинхронизирующиеся поточные шифры.....	47
14.3. Шифры гаммирования	50

14.4. Свойства криптографических протоколов поточного шифрования.....	50
14.4.1. Передача гаммы в линию связи.....	50
14.4.2. Повторное использование гаммы.....	51
14.4.3. Корреляционные атаки.....	52
14.4.4. Восстановление текста, зашифрованного неравновероятной гаммой.....	53
14.5. Криптографические генераторы.....	54
14.6. Критерии оценки криптографических свойств поточных шифров.....	64
<i>Контрольные вопросы и задания.....</i>	<i>65</i>
Глава 15. Симметричные блочные шифры	67
15.1. Сравнение характеристик асимметричных и симметричных блочных шифров.....	67
15.2. Принципы построения блочных шифров.....	67
15.2.1. Структура СБШ.....	67
15.2.2. Шифры Фейстеля.....	69
15.2.3. Построение цикловой функции.....	70
15.2.4. Входное и выходное отображения.....	72
15.2.5. Построение ключевого расписания.....	72
15.3. Слабые ключи итеративного шифра.....	73
15.4. Режимы шифрования.....	75
15.5. Усложнение симметричных блочных шифров, чередование.....	79
15.6. Аутентификация с помощью симметричных блочных шифров.....	81
<i>Контрольные вопросы и задания.....</i>	<i>82</i>
Глава 16. Хеш-функции и асимметричные криптосистемы.....	83
16.1. Хеш-функции.....	83
16.2. Шифрсистема RSA.....	84
16.3. Шифрсистема Эль-Гамала.....	86
16.4. Схема подписи Эль-Гамала.....	87
16.5. Аутентификация с помощью асимметричных криптосистем.....	87
16.6. Электронные платежные системы.....	88
16.7. Анализ криптосистем с открытым ключом.....	90
16.7.1. Распознавание простоты числа.....	90
16.7.2. Построение простых чисел.....	92
16.7.3. Задача факторизации.....	93
16.7.4. Задача дискретного логарифмирования.....	95
16.8. Криптосистемы на основе эллиптических кривых.....	97
<i>Контрольные вопросы и задания.....</i>	<i>99</i>
Глава 17. Ключевая подсистема криптосистемы	101
17.1. Строение и вероятностная модель ключевого множества.....	101
17.2. Случайность ключей.....	103
17.3. Секретность ключей.....	104
17.4. Распределение ключей.....	105
17.4.1. Генерация ключей на основе симметричных криптосистем.....	106
17.4.2. Генерация ключей на основе асимметричных криптосистем.....	108
17.5. Предварительное распределение ключей.....	110

17.6. Другие процедуры жизненного цикла ключей	111
17.7. Стойкость к компрометациям и архитектура ключевых систем	112
17.8. Особенности ключевых систем для передачи и для хранения данных	115
<i>Контрольные вопросы и задания</i>	116
Глава 18. Подходы к оценке стойкости криптосистем	117
18.1. О криптографической стойкости	117
18.2. Системный подход к оценке практической стойкости	117
18.3. Асимптотический анализ стойкости	120
18.4. Анализ на основе оценки количества шифрматериала	121
18.5. Стоимостный подход	121
18.6. Цели, содержание и условия криптографического анализа	122
18.7. Вычислительные средства криптоанализа	123
<i>Контрольные вопросы и задания</i>	126
 Раздел II ПРИКЛАДНЫЕ АСПЕКТЫ КРИПТОГРАФИИ 	
Глава 19. Криптография и информационная безопасность	129
19.1. Основные направления обеспечения информационной безопасности	129
19.1.1. Аутентификация и идентификация	129
19.1.2. Управление доступом (защита от НСД)	130
19.1.3. Обеспечение неотказуемости	131
19.1.4. Обеспечение конфиденциальности	133
19.1.5. Обеспечение целостности	133
19.1.6. Аудит и оповещение об опасности	134
19.2. Виды электронной подписи	136
19.3. Электронные аукционы	140
<i>Контрольные вопросы и задания</i>	141
Глава 20. Модели инфраструктуры открытых ключей	143
20.1. Переход от бумажного к электронному документообороту	143
20.2. Инфраструктуры открытых ключей	144
20.2.1. Компоненты PKI-инфраструктуры	146
20.2.2. Типы PKI-инфраструктур	147
20.2.3. Служба единого каталога	148
20.3. Североамериканская модель инфраструктуры открытых ключей	149
20.4. Западноевропейская модель инфраструктуры открытых ключей, подтверждения подлинности ЭП и сертификатов открытых ключей	154
20.5. Российская модель национальной инфраструктуры открытых ключей, подтверждения подлинности ЭП и сертификатов открытых ключей	157
<i>Контрольные вопросы и задания</i>	161
Глава 21. Криптографические методы защиты экономической информации	163
21.1. Новая «виртуальная социально-экономическая среда», «киберуязвимость»	163
21.2. Система электронной коммерции в сети Интернет	166

21.3. Характеристика IOTP-протокола	169
21.3.1. Общая структура (формат) IOTP-сообщения.....	171
21.3.2. Состав участников торговой сделки.....	172
21.3.3. Торговые процедуры	174
21.4. Характеристика RAPI-интерфейса	175
21.4.1. Структура RAPI-интерфейса	175
21.5. Принципы применения ЭП в IOTP/RAPI.....	178
<i>Контрольные вопросы и задания.....</i>	<i>180</i>
Глава 22. Системы аутентификации (идентификации)	181
22.1. Общие положения.....	181
22.1.1. Объекты и субъекты аутентификации.....	182
22.1.2. Формы аутентификации.....	182
22.1.3. Аутентификационная информация	182
22.1.4. Угрозы аутентификации.....	183
22.1.5. Гарантированность непрерывной аутентификации.....	184
22.1.6. Принципы, используемые при аутентификации	184
22.2. Основные схемы аутентификации	185
22.2.1. Аутентификация без привлечения доверенной третьей стороны.....	185
22.2.2. Аутентификация с привлечением доверенной третьей стороны	186
22.2.3. Доверие претендента к проверяющему	188
22.3. Способы АО с использованием алгоритмов симметричного шифрования.....	189
22.4. Аутентификация на основе применения электронной подписи	192
22.5. Аутентификация с использованием криптографической проверочной функции.....	194
22.6. Аутентификация на основе принципов «нулевого разглашения».....	195
22.6.1. Односторонняя аутентификация на основе параметров подлинности	197
22.6.2. Односторонняя аутентификация на основе целочисленной факторизации.....	198
22.6.3. Односторонняя аутентификация на основе дискретного логарифмирования, связанного с простыми или с составными числами	198
22.6.4. Односторонняя или обоюдная аутентификация на основе асимметричного шифрования.....	199
22.6.5. Односторонняя аутентификация на основе дискретного логарифмирования, связанного с эллиптическими кривыми	199
<i>Контрольные вопросы и задания.....</i>	<i>200</i>
Глава 23. Криптосистемы защиты речевых сообщений.....	201
23.1. Процесс воспроизведения речи и лингвистические свойства речи.....	201
23.2. Общие принципы защиты речевых сообщений.....	202
23.3. Аналоговые скремблеры	202
23.3.1. Аналоговые частотные скремблеры.....	203
23.3.2. Аналоговые временные скремблеры	206
23.3.3. Двумерные скремблеры	208

23.4. Цифровые системы защиты речи.....	211
23.4.1. Аналого-цифровые преобразования электрических сигналов. Представление сигналов в дискретном времени.....	211
23.4.2. ИКМ-преобразование.....	212
23.4.3. Разностное квантование аналоговых сигналов.....	217
23.4.4. Дельта-модуляция	218
23.4.5. Цифровое кодирование речевых сигналов с низкой скоростью....	221
<i>Контрольные вопросы и задания</i>	225
Глава 24. Системы шифрования факсимильных сообщений.....	226
24.1. Общие принципы передачи неподвижных изображений	226
24.2. Способы цифрового представления факсимильных сигналов	227
24.3. Адаптивное кодирование факсимильных сообщений.....	230
24.4. Двумерное кодирование факсимильных сообщений	233
24.5. Кодирование цветных факсимильных сообщений.....	236
24.6. Обеспечение конфиденциальности и целостности факсимильных сообщений	239
<i>Контрольные вопросы и задания</i>	239
Библиографический список	240
Ответы и решения	242
Предметный указатель.....	243