

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	3
Тема 1. ВВЕДЕНИЕ В КРИПТОЛОГИЮ .....	12
1.1. Основные понятия криптологии.....	12
1.2. История криптографии и традиционные системы шифрования.....	13
1.3. Классификация криптографических систем .....	25
1.4. Управление криптографическими ключами .....	27
1.5. Основные тенденции современной криптологии .....	28
Контрольные вопросы по теме .....	31
Тема 2. ПРЕОБРАЗОВАНИЯ МНОЖЕСТВ ЧИСЕЛ .....	33
2.1. Математическая логика.....	33
2.1.1. Высказывания и преобразования высказываний.....	33
2.1.2. Таблицы истинности .....	38
2.1.3. Условные высказывания.....	39
2.1.4. Эквивалентные высказывания .....	41
2.2. Основы теории множеств .....	44
2.2.1. Специальные виды множеств .....	46
2.2.2. Операции над множествами.....	47
2.2.3. Основные соотношения теории множеств.....	50
2.3. Комбинаторика.....	51
Контрольные вопросы по теме.....	54
Тема 3. АРИФМЕТИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ В КРИПТОСИСТЕМАХ .....	56
3.1. Элементарные арифметические соотношения.....	56
3.2. Операции над числами увеличенной разрядности .....	67
Контрольные вопросы по теме.....	74
Тема 4. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ КРИПТОСИСТЕМ И АНАЛИЗ АЛГОРИТМОВ.....	76
4.1. Основные алгебраические структуры.....	76
4.2. Функции и отображения .....	82
4.3. Структура конечных полей.....	85
4.4. Эллиптические кривые.....	87
4.2. Основы теории сложности алгоритмов.....	93
4.2.1. Асимптотические нотации.....	93
4.2.2. Классы сложности.....	95
Контрольные вопросы по теме.....	97
Тема 5. ВЕРОЯТНОСТНЫЕ ОСНОВЫ КРИПТОЛОГИИ .....	99
5.1. Основные понятия теории вероятностей .....	99
5.2. Основные теоремы теории вероятностей.....	103

5.3. Условная вероятность.....	105
5.4. Формулы полной вероятности и Байеса.....	107
5.5. Теорема о повторении опытов.....	107
5.6. Случайные величины и их характеристики.....	109
5.7. Числовые характеристики случайных величин.....	112
5.8. Моменты.....	114
5.9. Корреляционный момент и коэффициент корреляции.....	116
5.10. Основные распределения случайных величин, имеющие место в криптографических системах.....	117
Контрольные вопросы по теме.....	120
Тема 6. ВЕРОЯТНОСТНЫЕ МЕТОДЫ В КРИПТОЛОГИИ.....	122
6.1. Описание систем с помощью графов состояний.....	122
6.2. Марковские случайные процессы с дискретными состояниями и дискретным временем (марковские цепи).....	125
6.3. Основы теории информации.....	126
6.4. Энтропия сложной системы.....	130
6.5. Информация.....	132
6.6. Теоретическая стойкость криптосистем.....	134
6.6.1. Теория систем с совершенной секретностью.....	135
6.6.2. Шифр Вернама.....	136
6.6.3. Расстояние единственности шифра с секретным ключом.....	138
6.7. Идеальные криптосистемы.....	140
Контрольные вопросы по теме.....	142
Тема 7. ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИИ В КРИПТОСИСТЕМАХ.....	144
7.1. Системы счисления.....	144
7.2. Система остаточных классов.....	146
7.3. Двоичная система счисления.....	148
7.4. Шестнадцатеричная система счисления.....	148
7.5. Кодирование символов в информационных системах.....	149
7.5.1. ASCII.....	149
7.5.2. Кириллица.....	151
7.5.3. UNICODE.....	152
7.6. Вероятностное кодирование информации.....	153
7.6.1. Алгоритм Шеннона — Фано.....	156
7.6.2. Кодирование Хаффмана.....	158
7.6.3. Арифметическое кодирование.....	160
Контрольные вопросы по теме.....	163
Тема 8. ОСНОВЫ ПОСТРОЕНИЯ СТОЙКИХ ШИФРОВ.....	164
8.1. Основные примитивы симметричных криптосистем.....	164
8.1.1. Очистка.....	169
8.1.2. MDS.....	169
8.1.3. Псевдоадамаровское преобразование.....	169

8.1.4. Т-функции .....	170
8.2. Стохастические шифры .....	171
8.3. Преобразования асимметричных криптосистем .....	173
8.4. Вспомогательные алгоритмы асимметричных криптосистем .....	177
8.4.1. Нахождение простых чисел .....	177
8.4.2. Методы факторизации .....	182
8.4.3. Дискретное логарифмирование .....	188
Контрольные вопросы по теме .....	194
Тема 9. БЛОЧНЫЕ ШИФРЫ .....	196
9.1. Режимы использования блочных шифров .....	196
9.2. Режим электронной шифровальной книги .....	198
9.3. Режим сцепления блоков шифртекста .....	199
9.4. Режим обратной связи по шифртексту .....	200
9.5. Режим обратной связи по выходу .....	201
9.6. Режим счетчика .....	202
9.7. Вспомогательные процедуры .....	203
9.8. Настраиваемые шифры .....	206
9.9. Режим GSM .....	209
9.10. Режим ССМ .....	216
Контрольные вопросы по теме .....	221
Тема 10. ФАЙСТЕЛОВСКИЕ ШИФРЫ .....	223
10.1. Схема DES .....	223
10.2. Шифр Camellia .....	231
10.3. Шифр ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009) .....	236
10.4. Криптоанализ файстеловских шифров .....	239
10.4.1. Линейный криптоанализ .....	242
10.4.2. Построение линейной аппроксимации шифра .....	247
10.4.3. Извлечение битов ключа в линейном криптоанализе .....	249
10.4.4. Дифференциальный криптоанализ .....	250
10.4.5. Построение дифференциальных характеристик шифра .....	254
10.4.6. Извлечение битов ключа в дифференциальном криптоанализе .....	256
10.4.7. Разновидности дифференциального криптоанализа .....	257
Контрольные вопросы по теме .....	259
Тема 11. НЕФАЙСТЕЛОВСКИЕ ШИФРЫ .....	261
11.1. Схема Square .....	261
11.2. Реализация математических примитивов Square в Rijndael (AES) .....	262
11.3. Шифр Rijndael .....	266
11.4. Реализация инверсного шифра для Rijndael .....	274
11.5. Шифр SAFER .....	276
11.6. Высокопараллелизуемые шифры — Serpent .....	283
Контрольные вопросы по теме .....	288

Тема 12. КОНСТРУКЦИИ ХЭШ-ФУНКЦИЙ.....	289
12.1. Общий подход к разработке хэш-функций.....	289
12.2. Использование блочных шифров в качестве хэш-конструктивов.....	292
12.3. Whirlpool .....	294
12.3.1. Компоненты функции хэширования Whirlpool .....	294
12.3.2. Анализ безопасности Whirlpool.....	296
12.4. Семейство хэш-функций SHA .....	297
12.4.1. Константы SHA-2 .....	298
12.4.2. Алгоритм преобразования SHA-2.....	299
12.5. Высокоспараллелизуемые хэш-функции (на примере MD6).....	303
12.5.1. Основная стратегия преобразования .....	304
12.5.2. Режимы обработки данных .....	305
12.5.3. Управление преобразованием данных для различных режимов.....	307
12.6. Коды аутентичности сообщений.....	310
12.7. HMAC .....	311
Контрольные вопросы по теме.....	313
Приложение А. РЕАЛИЗАЦИЯ ОПЕРАЦИЙ НАД БОЛЬШИМИ ЧИСЛАМИ .....	314
ЛИТЕРАТУРА.....	334
АЛФАВИТНО-ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.....	342