

СОДЕРЖАНИЕ

ГЛАВА 1. ВВЕДЕНИЕ В КРИПТОГРАФИЮ	3
1.1. ВВЕДЕНИЕ	3
1.2. ИСТОРИЯ РАЗВИТИЯ КРИПТОГРАФИИ	7
1.3. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	30
ГЛАВА 2. ПОНЯТИЕ О ТРАДИЦИОННЫХ МЕТОДАХ ШИФРОВАНИЯ	35
2.1. МОДЕЛЬ ТРАДИЦИОННОГО ШИФРОВАНИЯ	35
2.2. ТРЕБОВАНИЯ К КРИПТОГРАФИЧЕСКИМ СИСТЕМАМ	41
2.3. КРАТКИЕ СВЕДЕНИЯ О КРИПТОАНАЛИЗЕ	42
2.4. КЛАССИФИКАЦИЯ МЕТОДОВ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ИНФОРМАЦИИ	44
ГЛАВА 3. ШИФРОВАНИЕ НА ОСНОВЕ МЕТОДОВ ПОДСТАНОВКИ	46
3.1. МОНОАЛФАВИТНЫЕ ШИФРЫ	46
3.2. ПОЛИАЛФАВИТНЫЕ ШИФРЫ	63
3.3. ТЕОРИЯ КРИПТОАНАЛИЗА ШИФРА ВИЖЕНЕРА	68
ГЛАВА 4. ШИФРОВАНИЕ НА ОСНОВЕ МЕТОДОВ ПЕРЕСТАНОВКИ	87
4.1. МЕТОДЫ ПЕРЕСТАНОВКИ	87
4.2. БЛОЧНЫЕ ШИФРЫ	89
4.3. РЕЖИМЫ ПРИМЕНЕНИЯ БЛОЧНЫХ ШИФРОВ	101
4.4. КОМПОЗИЦИОННЫЕ МЕТОДЫ ШИФРОВАНИЯ. КОМПОЗИЦИИ (КОМБИНАЦИИ) ШИФРОВ	105
ГЛАВА 5. СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ DES (DATA ENCRYPTION STANDARD)	106
5.1. ИСТОРИЯ СОЗДАНИЯ СТАНДАРТА DES	106
5.2.1. СХЕМА АЛГОРИТМА	110
5.2.2. НАЧАЛЬНАЯ ПЕРЕСТАНОВКА	110
5.2.4. ПЕРЕСТАНОВКА С РАСШИРЕНИЕМ	113
5.2.5. ПОДСТАНОВКА С ПОМОЩЬЮ S-БЛОКОВ	114

5.2.6. ПЕРЕСТАНОВКА С ПОМОЩЬЮ P-БЛОКОВ	117
5.2.7. ЗАКЛЮЧИТЕЛЬНАЯ ПЕРЕСТАНОВКА	118
5.3. ДЕШИФРОВАНИЕ DES	118
5.4. РЕЖИМЫ DES	119
5.5. АППАРАТНЫЕ И ПРОГРАММНЫЕ РЕАЛИЗАЦИИ DES	119
ГЛАВА 6. УПРАВЛЕНИЕ КЛЮЧАМИ В СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ	121
6.1. КРАТКАЯ ХАРАКТЕРИСТИКА КАНАЛЬНОГО И СКВОЗНОГО ШИФРОВАНИЯ	121
6.2. ПРИНЦИПЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ	124
6.3. ПРИНЦИПЫ УПРАВЛЕНИЯ КЛЮЧАМИ	129
6.3.1. УПРАВЛЕНИЕ ИЕРАРХИЕЙ КЛЮЧЕЙ	129
6.3.2. ДЕЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КЛЮЧАМИ	130
6.3.3. УПРАВЛЕНИЕ ИСПОЛЬЗОВАНИЕМ КЛЮЧЕЙ	131
ГЛАВА 7. СТОЙКОСТЬ КРИПТОГРАФИЧЕСКИХ СИСТЕМ И АЛГОРИТМОВ	134
7.1. ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКИЙ АНАЛИЗ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ	134
7.2. АНАЛИЗ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ НА ОСНОВЕ ТЕОРИИ СЛОЖНОСТИ	136
ГЛАВА 8. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ	142
8.1. ОБЩАЯ СХЕМА ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ	142
8.2. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ И АУТЕНТИФИКАЦИЯ В КРИПТОСИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ	146
8.3. ОСОБЕННОСТИ ПРИМЕНЕНИЯ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ	149
8.4. КРИПТОАНАЛИЗ СИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ	152
ГЛАВА 9. ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ЧИСЕЛ	154
9.1. ДЕЛИТЕЛИ И ПРОСТЫЕ ЧИСЛА	154
9.2. АРИФМЕТИКА В КЛАССАХ ВЫЧЕТОВ	158

9.3. ТЕОРЕМА ЭЙЛЕРА	160
9.4. ДИСКРЕТНЫЕ ЛОГАРИФМЫ	166
ГЛАВА 10. АЛГОРИТМ ШИФРОВАНИЯ RSA	170
10.1. СТРУКТУРА АЛГОРИТМА RSA	170
10.2. ВЫЧИСЛИТЕЛЬНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА RSA	173
10.2.1. ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ	173
10.2.2. ВЫЧИСЛЕНИЕ КЛЮЧЕЙ	174
10.3. КРИПТОАНАЛИЗ АЛГОРИТМА RSA	176
ГЛАВА 11. УПРАВЛЕНИЕ КЛЮЧАМИ В АСИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ	183
11.1. РАСПРЕДЕЛЕНИЕ ОТКРЫТЫХ КЛЮЧЕЙ	183
11.2. РАСПРЕДЕЛЕНИЕ СЕКРЕТНЫХ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ	188
11.2.1. ПРОСТОЕ РАСПРЕДЕЛЕНИЕ СЕКРЕТНЫХ КЛЮЧЕЙ	188
11.2.2. РАСПРЕДЕЛЕНИЕ СЕКРЕТНЫХ КЛЮЧЕЙ С ОБЕСПЕЧЕНИЕМ КОНФИДЕНЦИАЛЬНОСТИ И АУТЕНТИФИКАЦИИ	190
11.2.3. ГИБРИДНАЯ СХЕМА	191
11.2.4. ОБМЕН КЛЮЧАМИ ПО СХЕМЕ ДИФФИ – ХЕЛЛМАНА	191
ГЛАВА 12. ХЭШ-ФУНКЦИИ	196
12.1. ТРЕБОВАНИЯ К ХЭШ-ФУНКЦИЯМ	196
12.2. ПРОСТЫЕ ХЭШ-ФУНКЦИИ	197
12.3. ПАРАДОКС ДНЯ РОЖДЕНИЯ И АТАКИ, НА НЕМ ОСНОВАННЫЕ	200
12.4. СПОСОБЫ ИСПОЛЬЗОВАНИЯ ХЭШ-ФУНКЦИЙ	203
12.5. КРИПТОАНАЛИЗ ХЭШ-ФУНКЦИЙ	206
ГЛАВА 13. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ	208
13.1. ТРЕБОВАНИЯ К ЦИФРОВЫМ ПОДПИСЯМ И ИХ КЛАССИФИКАЦИЯ	208
13.1.1. ОБЩИЕ ПОЛОЖЕНИЯ	208
13.1.2. НЕПОСРЕДСТВЕННАЯ ЦИФРОВАЯ ПОДПИСЬ	210

13.1.3. АРБИТРАЖНАЯ ЦИФРОВАЯ ПОДПИСЬ	211
13.2. ОСНОВНЫЕ АЛГОРИТМЫ ЦИФРОВЫХ ПОДПИСЕЙ	214
ГЛАВА 14. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ	221
14.1. ВЗАИМНАЯ АУТЕНТИФИКАЦИЯ	221
14.2. ОДНОСТОРОННЯЯ АУТЕНТИФИКАЦИЯ	229
ГЛАВА 15. ИМИТОСТОЙКОСТЬ И ПОМЕХОУСТОЙЧИВОСТЬ КРИПТОСИСТЕМ	232
15.1. ОСНОВНЫЕ ПРИНЦИПЫ ИМИТОЗАЩИТЫ И ПОМЕХОУСТОЙЧИВОСТИ КРИПТОСИСТЕМ	232
15.2. СТРУКТУРА ИМИТОЗАЩИЩЕННОГО ПОМЕХОУСТОЙЧИВОГО КАНАЛА СВЯЗИ	233
15.3. ИМИТОЗАЩИТА НА ОСНОВЕ РЕЖИМА ВЫРАБОТКИ ИМИТОВСТАВКИ	235
ГЛАВА 16. МЕТОДЫ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ	237
16.1. ТРЕБОВАНИЯ К СЛУЧАЙНЫМ ЧИСЛОВЫМ ПОСЛЕДОВАТЕЛЬНОСТЯМ. ФИЗИЧЕСКИЕ ИСТОЧНИКИ СЛУЧАЙНЫХ ЧИСЕЛ	237
16.2. ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ	239
16.3. КРИПТОГРАФИЧЕСКИ ГЕНЕРИРУЕМЫЕ ПСЕВДОСЛУЧАЙНЫЕ ЧИСЛА	247
ГЛАВА 17. КРИПТОГРАФИЧЕСКИЕ ШИФРАТОРЫ	252
17.1. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ И СТРУКТУРА АППАРАТНОГО ШИФРАТОРА	252
17.2. ПРИНЦИП ДЕЙСТВИЯ АППАРАТНОГО ШИФРАТОРА	257
17.3. ОСНОВНЫЕ ТИПЫ СОВРЕМЕННЫХ ШИФРАТОРОВ	262
17.4. ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ТЕХНОЛОГИИ СМАРТ-КАРТ	265
ГЛАВА 18. ОСОБЕННОСТИ ПРОГРАММНО-АППАРАТНОЙ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ И СЕТЕЙ СВЯЗИ	268

18.1. ПРОХОДНЫЕ ШИФРАТОРЫ: СТРУКТУРА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	268
18.1.1. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ И СТРУКТУРА ПРОХОДНОГО ШИФРАТОРА	268
18.1.2. ЗАГРУЗКА КЛЮЧЕЙ ШИФРОВАНИЯ	269
18.1.3. ВЗАИМОДЕЙСТВИЕ ШИФРАТОРА С ПРОГРАММАМИ КОМПЬЮТЕРА	269
18.1.4. ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ	271
18.2. ОРГАНИЗАЦИЯ КРИПТОЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ ТЕЛЕФОННОЙ, МОБИЛЬНОЙ И СПЕЦИАЛЬНОЙ СВЯЗИ	273
18.3. СПЕЦИАЛИЗИРОВАННЫЕ ШИФРАТОРЫ	277
ГЛАВА 19. КРИПОСИСТЕМЫ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ	284
19.1. АЛГОРИТМЫ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ	284
19.2. ПРОЦЕДУРА СОЗДАНИЯ КЛЮЧЕЙ	302
19.3. ШИФРОВАНИЕ И ДЕШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЛИПТИЧЕСКИХ КРИВЫХ	306
19.4. КРИПОСИСТЕМЫ ЭЛЬ-ГАМАЛЯ, ОСНОВАННЫЕ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ	308
БИБЛИОГРАФИЧЕСКИЙ СПИСОК	312