

СОДЕРЖАНИЕ

Тема 13. ГЕНЕРАТОРЫ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЧИСЕЛ.....	7
13.1. Последовательности чисел.....	7
13.2. Простейшие программные генераторы.....	9
13.3. Простейшие аппаратные генераторы.....	11
13.4. XORShift-генератор.....	14
13.5. Криптографические ГПСП.....	17
13.5.1. Генератор на основе Rijndael.....	18
13.5.2. Dual Elliptic Curve Deterministic RBG (Dual_EC_DRBG).....	18
13.6. Генерация истинно случайных последовательностей чисел.....	23
13.7. Реализация ГПСП.....	25
13.8. Тесты качества генераторов последовательностей чисел.....	29
Контрольные вопросы по теме.....	43
Тема 14. ПРОГРАММНЫЕ ШИФРЫ.....	45
14.1. Общие принципы построения программных шифров.....	45
14.2. Представление криптографических преобразований в виде отображений и подстановок.....	47
14.2.1. Криптосистема с перестановкой фиксированных процедур.....	47
14.2.2. Многопроходные криптосистемы с гибким алгоритмом.....	48
14.3. Шифр Twofish.....	49
14.3.1. Функция F	51
14.3.2. Функция g	52
14.3.3. Процедура формирования расширенного ключа.....	52
14.3.4. Функция h	54
14.3.5. Таблицы подстановки, зависящие от ключа.....	55
14.3.6. Слова расширенного ключа.....	55
14.3.7. Перестановки q_0 и q_1	56
14.4. Шифр RC6.....	57
14.4.1. Формирование раундовых ключей.....	58
14.4.2. Шифрование.....	60
14.4.3. Расшифрование.....	63
14.5. Комбинирование классических и современных техник криптопреобразований — шифр MARS.....	63
14.5.1. Высокоуровневая структура.....	64
14.5.2. Выбор операций.....	66
Контрольные вопросы по теме.....	74
Тема 15. ПОТОКОВЫЕ КРИПТОСИСТЕМЫ.....	76
15.1. Общий подход к проектированию потоковых шифров.....	76
15.2. Использование LFSR в качестве примитива потокового шифра.....	77
15.3. Генератор Геффа.....	80

15.4. Использование сдвиговых регистров в алгоритмах шифрования в системе защиты сотовых сетей стандарта GSM.....	81
15.5. Рандомизированные сдвиговые регистры с обратной связью.....	86
15.6. RC4	87
15.7. Шифр SNOW	88
15.7.1. Элементы шифра SNOW 2.0	90
15.7.2. Инициализация ключа	91
15.8. Комплекс шифров VEST.....	92
15.9. Шифр Salsa20.....	98
15.10. Шифр HC-256	100
Контрольные вопросы по теме.....	103
Тема 16. РЕАЛИЗАЦИИ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ.....	104
16.1. Формирование общего ключа по Диффи — Хеллману.....	104
16.2. Криптосистема RSA	105
16.3. Реализация криптосистемы RSA.....	106
16.3.1. Преобразования, используемые в RSA PKCS #1	108
16.3.2. Схемы шифрования	108
16.3.3. Схема OAEP	114
16.4. Построение асимметричных криптосистем на эллиптических кривых.....	115
16.5. Гибридное шифрование.....	116
16.5.1. Криптосистема ACE-KEM.....	120
16.5.2. ECIES	121
16.5.3. ECIES-KEM	123
16.5.4. EPOC-2	124
Контрольные вопросы по теме.....	126
Тема 17. ЦИФРОВЫЕ ПОДПИСИ.....	128
17.1. Схема электронной цифровой подписи	128
17.2. Подпись по Эль-Гамало.....	130
17.3. Схема Шнорра	132
17.4. Стандарт цифровой подписи DSS	132
17.4.1. Алгоритм DSA.....	133
17.4.2. ECDSA.....	134
17.5. Современный вариант российского стандарта ЭЦП	137
17.6. Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002.....	139
17.7. ЭЦП на основе симметричной криптосистемы	142
17.8. Проблемы распространения открытых ключей.....	143
17.9. Использование сертификатов.....	146
17.10. Инфраструктура открытого ключа	149
17.10.1. Структура сертификата.....	150
17.10.2. Классы сертификатов	152
17.10.3. Цепочки сертификатов.....	152

17.10.4. Этапы внедрения инфраструктуры открытого ключа	154
17.10.5. Стандарты инфраструктуры открытого ключа	155
Контрольные вопросы по теме.....	157
Тема 18. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ	159
18.1. Классификация криптографических протоколов.....	159
18.2. Протоколы нулевого разглашения знаний.....	163
18.3. Протоколы разделения общего секрета.....	164
18.3.1. Верифицируемые схемы разделения секрета.....	168
18.3.2. Разделение секрета в системах с пролонгированной безопасностью.....	169
18.4. Протоколы формирования электронной цифровой подписи.....	170
18.5. Протокол слепой цифровой подписи	172
18.6. Протоколы аутентификации в телекоммуникациях	174
18.6.1. Протокол Kerberos	177
18.6.2. Протокол PAP	179
18.6.3. Протокол CHAP.....	180
18.6.4. Протокол EAP	182
18.7. Управление ключами в современных телекоммуникационных системах	184
Контрольные вопросы по теме.....	186
Тема 19. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ	188
19.1. Выбор надежных криптографических алгоритмов	188
19.2. Теория дискового шифрования	189
19.3. Защита виртуальной памяти компьютера.....	192
19.4. Концепция Trusted Computing	193
19.5. Модуль доверительной платформы	195
19.6. Реализация доверительной платформы в Windows NT 6.....	197
19.7. Криптопровайдеры CRYPTOAPI.....	199
19.8. Реализация защищенной файловой системы в Windows NT 5.....	201
19.9. Microsoft BitLocker	204
19.10. Реализация устройств криптографической защиты.....	209
19.11. Криптографические интерфейсы следующего поколения в Windows NT 6	211
Контрольные вопросы по теме.....	213
Тема 20. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ.....	216
20.1. Общий подход к внедрению функций криптографической защиты в рамках операционных систем.....	216
20.2. Реализация криптографических подсистем	217
20.3. Криптографическая защита транспортного уровня.....	219
20.4. Криптографическая защита прикладного уровня	222

20.5. Технология защищенного канала	223
20.6. Стек протоколов IP Security	231
Контрольные вопросы по теме.....	240
Тема 21. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ.....	241
21.1. Беспроводные сети стандарта IEEE 802.11	241
21.2. Задачи информационной безопасности в рамках беспроводной сети.....	245
21.3. Обзор средств обеспечения информационной безопасности до RSN IEEE 802.11.....	246
21.3.1. Шифрование	249
21.3.2. Целостность данных.....	253
21.3.3. Защита от повтора	255
21.3.4. Доступность.....	255
21.4. Краткий обзор безопасности IEEE 802.11i	255
21.5. Создание защищенных систем на основе стандарта 802.11i	257
21.5.1. Фазы операций IEEE 802.11 RSN	258
21.5.2. Иерархии ключей, механизмы управления и распространения ключей.....	261
21.5.3. Протоколы обеспечения конфиденциальности и целостности в RSN.....	264
21.5.4. Протокол формирования кода аутентичности сообщения на основе комбинации режима счетчика и сцепления блоков шифртекста	268
Контрольные вопросы по теме.....	273
Приложение Б. ТЕРМИНЫ СТАНДАРТА FIPS-140-3	275
ЛИТЕРАТУРА	285
АЛФАВИТНО-ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	292