

ОГЛАВЛЕНИЕ

Предисловие	3
1. Введение	4
Задачи и упражнения	10
2. Криптосистемы с открытым ключом	11
2.1. Предыстория и основные идеи	11
2.2. Первая система с открытым ключом — система Диффи–Хеллмана	17
2.3. Элементы теории чисел	20
2.4. Шифр Шамира	27
2.5. Шифр Эль-Гамала	30
2.6. Односторонняя функция с «лазейкой» и шифр RSA	33
Задачи и упражнения	37
Темы лабораторных работ	39
3. Методы взлома шифров, основанных на дискретном логарифмировании	40
3.1. Постановка задачи	40
3.2. Метод «шаг младенца, шаг великана»	42
3.3. Алгоритм исчисления порядка	44
Задачи и упражнения	49
Темы лабораторных работ	50
4. Электронная, или цифровая подпись	51
4.1. Электронная подпись RSA	51
4.2. Электронная подпись на базе шифра Эль-Гамала	54
4.3. Стандарты на электронную (цифровую) подпись	57
Задачи и упражнения	62
Темы лабораторных работ	63

5. Криптографические протоколы	65
5.1. Ментальный покер	65
5.2. Доказательства с нулевым знанием	70
Задача о раскраске графа	71
Задача о нахождении гамильтонова цикла в графе	74
5.3. Электронные деньги	82
5.4. Взаимная идентификация с установлением ключа	88
Задачи и упражнения	94
Темы лабораторных работ	96
6. Криптосистемы на эллиптических кривых	97
6.1. Введение	97
6.2. Математические основы	98
6.3. Выбор параметров кривой	106
6.4. Построение криптосистем	108
Шифр Эль-Гамала на эллиптической кривой	109
Цифровая подпись по ГОСТ Р 34.10-2012	110
Алгоритм ECDSA	111
6.5. Эффективная реализация операций	112
6.6. Определение количества точек на кривой	118
6.7. Использование стандартных кривых	127
Задачи и упражнения	130
Темы лабораторных работ	130
7. Теоретическая стойкость криптосистем	132
7.1. Введение	132
7.2. Теория систем с совершенной секретностью	133
7.3. Шифр Вернама	135
7.4. Элементы теории информации	137
7.5. Устойчивость шифра Вернама к небольшим отклонениям ключа от случайности	143
7.6. Шифры с бегущим ключом	148
7.7. Расстояние единственности шифра с секретным ключом	152
7.8. Идеальные криптосистемы	158
Задачи и упражнения	164

8. Современные шифры с секретным ключом	166
8.1. Введение	166
8.2. Блочные шифры	169
Шифр Магма	171
Шифр RC6	174
Шифр Rijndael (AES)	177
Шифр Кузнечик	189
8.3. Основные режимы функционирования блочных шифров	195
Режим ECB	196
Режим CBC	197
8.4. Поточковые шифры	197
Режим OFB блочного шифра	199
Режим CTR блочного шифра	201
Алгоритм RC4	201
Алгоритм HC-128	203
8.5. Криптографические хеш-функции	206
9. Криптовалюты и блокчейн	216
9.1. Введение	216
9.2. Доказательство выполнения работы (proof-of-work) и Хэшкэш (Hashcash)	216
9.3. Датирование документов (time-stamping)	220
9.4. Блокчейн (blockchain)	223
9.5. Биткоин (bitcoin) и криптовалюты	227
Транзакции и биткоины	228
Формирование бухгалтерской книги и производство биткоинов	230
Надежность системы биткоин	233
10. Случайные числа в криптографии	234
10.1. Введение	234
10.2. Задачи, возникающие при использовании физических генераторов случайных чисел	236
10.3. Генераторы псевдослучайных чисел	238
10.4. Тесты для проверки генераторов случайных и псевдослучайных чисел	241
10.5. Статистическая атака на блочные шифры	246
10.6. Атака различения на поточковые шифры	258

11. Стеганография и стегоанализ	261
11.1. Назначение и применение стеганографии в современных информационных технологиях	261
11.2. Основные методы встраивания скрытых данных	267
11.3. Стегоанализ на основе сжатия данных	272
11.4. Асимптотически оптимальные совершенные стеганографические системы	274
Ответы к задачам и упражнениям	284
Список литературы	288