

# ОГЛАВЛЕНИЕ

<b>Предисловие</b> . . . . .	<b>3</b>
<b>1. Введение</b> . . . . .	<b>5</b>
Задачи и упражнения . . . . .	11
<b>2. Криптосистемы с открытым ключом</b> . . . . .	<b>12</b>
2.1. Предыстория и основные идеи . . . . .	12
2.2. Первая система с открытым ключом — система Диффи–Хеллмана . . . . .	18
2.3. Элементы теории чисел . . . . .	21
2.4. Шифр Шамира . . . . .	28
2.5. Шифр Эль-Гамала . . . . .	31
2.6. Односторонняя функция с «лазейкой» и шифр RSA . . . . .	34
Задачи и упражнения . . . . .	38
Темы лабораторных работ . . . . .	40
<b>3. Методы взлома шифров, основанных на дискретном логарифмировании</b> . . . . .	<b>41</b>
3.1. Постановка задачи . . . . .	41
3.2. Метод «шаг младенца, шаг великана» . . . . .	43
3.3. Алгоритм исчисления порядка . . . . .	45
Задачи и упражнения . . . . .	50
Темы лабораторных работ . . . . .	51
<b>4. Электронная, или цифровая подпись</b> . . . . .	<b>52</b>
4.1. Электронная подпись RSA . . . . .	52
4.2. Электронная подпись на базе шифра Эль-Гамала . . . . .	55
4.3. Стандарты на электронную (цифровую) подпись . . . . .	58
Задачи и упражнения . . . . .	62
Темы лабораторных работ . . . . .	64

<b>5. Криптографические протоколы . . . . .</b>	<b>65</b>
5.1. Ментальный покер . . . . .	65
5.2. Доказательства с нулевым знанием . . . . .	70
Задача о раскраске графа . . . . .	71
Задача о нахождении гамильтонова цикла в графе . . . . .	75
5.3. Электронные деньги . . . . .	82
5.4. Взаимная идентификация с установлением ключа . . . . .	88
Задачи и упражнения . . . . .	95
Темы лабораторных работ . . . . .	96
<b>6. Криптосистемы на эллиптических кривых . . . . .</b>	<b>97</b>
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 Р34.10-2001 . . . . .	110
6.5. Эффективная реализация операций . . . . .	111
6.6. Определение количества точек на кривой . . . . .	117
6.7. Использование стандартных кривых . . . . .	126
Задачи и упражнения . . . . .	129
Темы лабораторных работ . . . . .	129
<b>7. Теоретическая стойкость криптосистем . . . . .</b>	<b>131</b>
7.1. Введение . . . . .	131
7.2. Теория систем с совершенной секретностью . . . . .	132
7.3. Шифр Вернама . . . . .	134
7.4. Элементы теории информации . . . . .	135
7.5. Расстояние единственности шифра с секретным ключом	142
7.6. Идеальные криптосистемы . . . . .	148
Задачи и упражнения . . . . .	154
<b>8. Современные шифры с секретным ключом . . . . .</b>	<b>156</b>
8.1. Введение . . . . .	156
8.2. Блочные шифры . . . . .	159
Шифр ГОСТ 28147-89 . . . . .	161
Шифр RC6 . . . . .	164
Шифр Rijndael (AES) . . . . .	167

8.3. Основные режимы функционирования блочных шифров . . . . .	177
Режим ECB . . . . .	177
Режим CBC . . . . .	178
8.4. Поточковые шифры . . . . .	179
Режим OFB блочного шифра . . . . .	181
Режим CTR блочного шифра . . . . .	182
Алгоритм RC4 . . . . .	183
8.5. Криптографические хеш-функции . . . . .	185
<b>9. Случайные числа в криптографии . . . . .</b>	<b>188</b>
9.1. Введение . . . . .	188
9.2. Задачи, возникающие при использовании физических генераторов случайных чисел . . . . .	190
9.3. Генераторы псевдослучайных чисел . . . . .	192
9.4. Тесты для проверки генераторов случайных и псевдослучайных чисел . . . . .	195
9.5. Статистическая атака на блочные шифры . . . . .	200
<b>Ответы к задачам и упражнениям . . . . .</b>	<b>214</b>
<b>Список литературы . . . . .</b>	<b>218</b>
<b>Предметный указатель . . . . .</b>	<b>222</b>