ОГЛАВЛЕНИЕ

Предисловие 3

1. Введение 5

2. Криптосистемы с открытым ключом 12
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-Гамаля 31
2.6. Односторонняя функция с «лазейкой» и шифр RSA . . 34

3. Методы взлома шифров, основанных на дискретном логарифмировании 38
3.1. Постановка задачи 38
3.2. Метод «шаг младенца, шаг великана» 40
3.3. Алгоритм исчисления порядка 42

4. Электронная, или цифровая подпись 48
4.1. Электронная подпись RSA 48
4.2. Электронная подпись на базе шифра Эль-Гамаля . . . 51
4.3. Стандарты на электронную (цифровую) подпись 54

5. Криптографические протоколы 59
5.1. Ментальный покер 59
5.2. Доказательства с нулевым знанием 64
Задача о раскраске графа 65
Задача о нахождении гамильтонова цикла в графе . . . 68
5.3. Электронные деньги 76
5.4. Взаимная идентификация с установлением ключа . . . 82

6. Криптосистемы на эллиптических кривых 89
6.1. Введение 89
6.2. Математические основы 90
6.3. Выбор параметров кривой 98
6.4. Построение криптосистем 100
Шифр Эль-Гамаля на эллиптической кривой 101
Цифровая подпись по ГОСТ Р34.10-2001 102
6.5. Эффективная реализация операций 103
6.6. Определение количества точек на кривой 109
6.7. Использование стандартных кривых 118

7. Теоретическая стойкость криптосистем 121
7.1. Введение 121
7.2. Теория систем с совершенной секретностью 122
7.3. Шифр Вернама 124
7.4. Элементы теории информации 125
7.5. Расстояние единственности шифра с секретным ключом 132
7.6. Идеальные криптосистемы 138

8. Современные шифры с секретным ключом 145
8.1. Введение 145
8.2. Блоковые шифры 148
Шифр ГОСТ 28147-89 150
Шифр RC6 153
Шифр Rijndael (AES) 156
8.3. Основные режимы функционирования блоковых шифров 166
Режим ECB 166
Режим CBC 167
8.4. Потоковые шифры 168
Режим OFB блокового шифра 170
Режим CTR блокового шифра 171
Алгоритм RC4 172
8.5. Криптографические хеш-функции 174

9. Случайные числа в криптографии 177
9.1. Введение 177
9.2. Задачи, возникающие при использовании физических генераторов случайных чисел 179