ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ 5

Глава 1. ВВЕДЕНИЕ 7

Глава 2. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ 14
- 2.1 Предыстория и основные идеи 14
- 2.2 Первая система с открытым ключом 21
- 2.3 Элементы теории чисел 24
- 2.4 Шифр Шамира 30
- 2.5 Шифр Эль-Гамаля 33
- 2.6 Односторонняя функция с "лазейкой" и шифр RSA 35

Глава 3. МЕТОДЫ ВЗЛОМА ШИФРОВ 40
- 3.1 Постановка задачи 40
- 3.2 Метод "Шаг младенца — шаг великана" 42
- 3.3 Алгоритм исчисления порядка 44

Глава 4. ЭЛЕКТРОННАЯ, ИЛИ ЦИФРОВАЯ ПОДПИСЬ 49
- 4.1 Электронная подпись RSA 49
- 4.2 Электронная подпись на базе шифра Эль-Гамаля 52
- 4.2 Стандарты на электронную (цифровую) подпись 55

Глава 5. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ 60
- 5.1 Ментальный покер 61
- 5.2 Доказательства с нулевым знанием 65
  - 5.2.1 Задача о раскраске графа 66
  - 5.2.2 Задача о нахождении гамильтонова цикла в графе . . 69
- 5.3 Электронные деньги 76
- 5.4 Взаимная идентификация с установлением ключа 81

Глава 6. КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ **86**
6.1 Введение 86
6.2 Математические основы 87
6.3 Выбор параметров кривой 94
6.4 Построение криптосистем 97
6.4.1 Шифр Эль-Гамаля на эллиптической кривой 97
6.4.2 Цифровая подпись на эллиптической кривой (ГОСТ Р34.10-2001) 98
6.5 Эффективная реализация операций 99
6.6 Определение количества точек на кривой 105
6.7 Использование стандартных кривых 114

Глава 7. ТЕОРЕТИЧЕСКАЯ СТОЙКОСТЬ КРИПТОСИСТЕМ **117**
7.1 Введение 117
7.2 Теория систем с совершенной секретностью 118
7.3 Шифр Вернама 120
7.4 Элементы теории информации 121
7.5 Расстояние единственности с секретным ключом 128
7.6 Идеальные криптосистемы 132

Глава 8. СОВРЕМЕННЫЕ ШИФРЫ С СЕКРЕТНЫМ КЛЮЧОМ **139**
8.1 Введение 139
8.2 Блоковые шифры 142
8.2.1 Шифр ГОСТ 28147-89 144
8.2.2 Шифр RC6 146
8.2.3 Шифр Rijndael (AES) 150
8.3 Режимы функционирования блоковых шифров 159
8.3.1 Режим ECB 160
8.3.2 Режим CBC 160
8.4 Потоковые шифры 161
8.4.1 Режим OFB блокового шифра 163
8.4.2 Режим CTR блокового шифра 164
8.4.3 Алгоритм RC4 165
8.5 Криптографические хеш-функции 167

Литература **170**