

*Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004. -- 173с.*

*ISBN 5-89176-233-1*

*В монографии изложены основные подходы и методы современной криптографии для решения задач, возникающих при обработке, хранении и передаче информации. Основное внимание уделено новым направлениям криптографии, связанным с обеспечением конфиденциальности взаимодействий пользователей компьютеров и компьютерных сетей. Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блочные и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо не скрываемых криптосистем и криптографии на эллиптических кривых. Изложение теоретического материала ведется достаточно строго, но с использованием довольно элементарного математического аппарата. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов.*

*Книга предназначена студентам и инженерам, работающим в области информационных технологий.*

# ОГЛАВЛЕНИЕ

<b>ПРЕДИСЛОВИЕ</b>	<b>5</b>
<b>Глава 1. ВВЕДЕНИЕ</b>	<b>7</b>
<b>Глава 2. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ</b>	<b>14</b>
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-Гамала .....	33
2.6 Односторонняя функция с "лазейкой" и шифр RSA .....	35
<b>Глава 3. МЕТОДЫ ВЗЛОМА ШИФРОВ</b>	<b>40</b>
3.1 Постановка задачи.....	40
3.2 Метод "Шаг младенца — шаг великана".....	42
3.3 Алгоритм исчисления порядка .....	44
<b>Глава 4. ЭЛЕКТРОННАЯ, ИЛИ ЦИФРОВАЯ ПОДПИСЬ</b>	<b>49</b>
4.1 Электронная подпись RSA .....	49
4.2 Электронная подпись на базе шифра Эль-Гамала .....	52
4.2 Стандарты на электронную (цифровую) подпись .....	55
<b>Глава 5. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ</b>	<b>60</b>
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

<b>Глава 6. КРИПТОСИСТЕМЫ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ</b>	<b>86</b>
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-Гамала 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
<b>Глава 7. ТЕОРЕТИЧЕСКАЯ СТОЙКОСТЬ КРИПТОСИСТЕМ</b>	<b>117</b>
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
<b>Глава 8. СОВРЕМЕННЫЕ ШИФРЫ С СЕКРЕТНЫМ КЛЮЧОМ</b>	<b>139</b>
8.1 Введение .....	139
8.2 Блочные 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 блочных шифров.....	159
8-3.1 Режим ECB.....	160
8.3.2 Режим CBC .....	160
8.4 Поточковые шифры.....	161
8.4.1 Режим OFB блочного шифра.....	163
8.4.2 Режим CTR блочного шифра .....	164
8.4.3 Алгоритм RC4.....	165
8.5 Криптографические хеш-функции .....	167
<b>Литература</b>	<b>170</b>