

СОДЕРЖАНИЕ

Конверт без обратного адреса	3
------------------------------------	---

Глава 1.

Информация нуждается в защите	5
Основные элементы кодирования.....	6
Принцип Керкгоффа.....	11
Телеграмма германскому послу	13

Глава 2.

Криптография от античных времен до XIX столетия	18
Скрытые послания.....	18
Транспозиционная криптография	21
Шифр Цезаря	24
Модульная арифметика и шифр Цезаря	28
Шпионские игры.....	36
Вне аффинного шифра.....	38
Частотный анализ	41
Шифр Марии Стюарт	45
Вклад Альберти.....	47
Первая система полиалфавитного шифра ...	48
«Черные кабинеты».....	54
Неизвестный криптоаналитик.....	56
Приложение 1	59

Глава 3.**История шифрования на Руси..... 64**

Самое простое — использовать малоизвестный алфавит.....	64
А если изменить кириллические буквы?.....	66
Но ведь знаки для замены букв можно придумать и специально!	69
«Флопяцевская азбука», «азбука копцева» и другие шифры	73
А почему бы кириллицу не заменить... кириллицей?	80
Воспользуемся цифирью	85
Не связать ли нам шифровочку?	86
Подведем итоги	87

Глава 4.**Шифровальные машины 88**

Алфавит точек и тире.....	88
Недалеко от Парижа.....	94
Машина «Энигма».....	98
Взлом шифра машины «Энигма»	103
Эстафету принимают англичане	107
Шифры других стран	110
Закодированные разговоры индейцев навахо	110
Шифр Хилла	111
Приложение 2.....	116

Глава 5.**Общение при помощи нуля и единицы..... 119**

Код ASCII.....	120
Шестнадцатеричная система	121
Системы счисления и замена основания ...	125
Как можно измерить информацию?	126
Кодирование в промышленных и торговых стандартах.....	133
Кредитные карты	133
Штрих-коды	138
Штрих-код EAN-13	140

Криптография открытых ключей ... 145

Проблема перехвата ключей 146

Алгоритм Диффи-Хеллмана..... 147

На помощь приходят простые числа 152

Алгоритм RSA..... 153

Почему алгоритм RSA надежен? 156

Разумная секретность 157

Удостоверение подлинности
сообщений и ключей 159

Хэш-подпись 161

Сертификаты открытых ключей 163

Безопасность интернет-магазинов 163

Приложение 3..... 165

Глава 7.**Квантовая криптография 170**

Вычисляем квантами 170

Странная кошка 173

Биты и кубиты 175

Неужели криптографии конец?..... 178

Кто нам мешает, тот и поможет 180

Этот шифр не одолеть 182

От сантиметров к километрам
абсолютной секретности 188**Послесловие редактора.****Фрактальное кодирование 190**