СОДЕРЖАНИЕ

Глава I. Кодирование и шифрование 5

От осколка — к кубиту. 6
Код и шифр 8
Сколько нужно ключей?. 10
Принцип Керкгоффса 11
Телеграмма германскому послу. 13

Глава 2. Криптография от античных времен. 19

Спарта против Афин 22
Отец аналитической криптографии 24
Аль-Кинди: взлом шифра 28
Шифрование слова Божьего. 30
Частотный анализ на практике 31
Руководство для юных леди 32
Шифровка из «Золотого жука» 33
Шрифт Марии Стюарт 35
Прорыв Альберти. 37
Диск Альберти 39
Квадрат Виженера 40
Шифр Гронсфельда 45
Криптографы при дворе «Короля Солнце» . . . 47
Неизвестный криптоаналитик. 48
Криптоаналитик Шерлок Холмс
и метод подбора. 51

Удивительная решетка. 52
От криптографии — к стенографии 54
Кино и кодирование 55
Шифровки в траншеях. 56

Глава 3. История шифрования на Руси 57

Самое простое —
использовать малоизвестный алфавит. 59
Но ведь знаки для замены букв
можно и придумать! 63
«Флопяцевская азбука»,
«Азбука Копцева» и другие. 67
А почему бы кириллицу не заменить...
кириллицей? 75
Воспользуемся цифирью 80
Не связать ли нам шифровочку? 81

Глава 4. Шифровальные машины 83

Азбука Морзе. 84
Невербальная связь 91
Шифр Плейфера 92
Недалеко от Парижа 95
Машина «Энигма» 99
Взлом шифра машины «Энигма» 104
Эстафету принимают англичане 107
Шифр Хилла. 111
Криптографические протоколы 114

Глава 5. Общение при помощи нолей и единиц 115
Двоичный бинарный код 116
Код ASCII 117
Шестнадцатеричная система 119
Системы счисления и замена основания . . . 123
Как измерить информацию 125
Протокол для безопасной передачи 130

Глава 6. Кодирование в промышленных и торговых масштабах 131
Первые штрихкоды 137
Штрихкод EAN-13 138
Коды QR 142
Простые числа и малая теорема Ферма 143

Глава 7. Криптография с использованием компьютера 145
Как безопасно распределить ключи? 148
На помощь приходят простые числа 153
Надёжный алгоритм RSA 155
Удостоверение подлинности сообщений и ключей. 160
Хэш-подпись 162
Сертификаты открытых ключей. 164
Шифрование во вред 166
Шифрование с помощью операции «XOR» . . 167

Симметричное шифрование. 168
Асимметричное шифрование 169
Шифрование с использованием нескольких ключей 171

Глава 8. Квантовая криптография 173
Немного квантовой теории 174
Биты и кубиты 185
Вычисляем квантами 188
Передача информации по квантовым каналам. 189
Передача сигнальных состояний. 192
Квантовые коды коррекции ошибок 194
Как избежать подслушивания 197
Квантовые измерения 199
Квантовая телепортация 204
Стратегии подслушивателя. 212
Этот шифр не одолеть 216

Глава 9. И, наконец, что же это — квантовый компьютер? 223
Возможность создания квантового компьютера. 226
Устройство квантового компьютера. 227
Квантовые компьютеры сегодня 231
Взгляд в будущее 233