

УДК 001, 501, 510  
ББК 22.1  
А56

**Альбов А. С.**  
А56 Квантовая криптография / Александр Альбов. —  
СПб.: Страта, 2015. — 248 с., с илл. — (серия  
«Просто»)

ISBN 978-5-906150-35-6

Криптография существует уже несколько тысяч лет. Мастерство шифрования и дешифровки было востребованным издревле и в разных целях, будь то тайная любовная переписка монарших особ или радиogramмы военных разведчиков из вражеского тыла. Книга рассказывает об истории этой шпионской науки, парадоксах и витках в ее развитии, приведших к новым революционным открытиям; об ученых, внесших мировой вклад в криптографическое дело.

Сегодня, когда информация приобретает едва ли не главную коммерческую ценность и политическое значение, искусство криптографии становится мощным средством в борьбе за влияние и превосходство. Грядет новый и решающий этап в эволюции вычислительных систем: эпоха квантовых компьютеров. Уже очень скоро информация, хранимая в наших базах данных, устремится в совсем другую реальность, странный и таинственный мир, открытый для нас Максом Планком век назад. Мир, в котором правят иные законы физики и живут иные частицы, делая его столь привлекательным для сокровенных человеческих тайн. Итак, мы снова ждем ответа на вопрос: грядет ли окончательная победа шифрования над дешифровкой в свете ожидаемого появления квантовых компьютеров?

Все права защищены. Никакая часть настоящей книги не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, а также размещение в Интернете, если на то нет письменного разрешения владельцев.

All rights reserved. No parts of this publication can be reproduced, sold or transmitted by any means without permission of the publisher.

УДК 001, 501, 510  
ББК 22.1

ISBN 978-5-906150-35-6

© Альбов А. С., 2015, текст  
© Ляпунов М. В., 2015, рисунки  
© Ляпунов М. В., 2015, обложка  
© ООО «Страта», 2015

## СОДЕРЖАНИЕ



<b>Глава 1.</b>	
<b>Основные элементы кодирования . . . . .</b>	<b>7</b>
Сколько нужно ключей? . . . . .	11
Принцип Керкгоффа . . . . .	13
Доктор Огюст Керкгоффс . . . . .	14
<b>Глава 2.</b>	
<b>Криптография от античных времён до XIX столетия . . . . .</b>	<b>17</b>
Скрытые послания . . . . .	19
Стеганография наших дней . . . . .	21
Транспозиционная криптография . . . . .	22
Руководство для юных леди . . . . .	24
Шифр Цезаря . . . . .	25
Кино и кодирование . . . . .	26
Евклид . . . . .	27
Шифр Полибия . . . . .	28
Шифрование слова Божьего . . . . .	29
Частотный анализ . . . . .	30
Аль-Кинди . . . . .	31
Криптоаналитик Шерлок Холмс и метод подбора . . . . .	33
Шифровка из «Золотого жука» . . . . .	34
Шифр Марии Стюарт . . . . .	36
Вклад Альберти . . . . .	38
Квадрат Виженера . . . . .	39
Леон Баттиста Альберти . . . . .	39
Блез де Виженер . . . . .	42
Дисковые игры . . . . .	44
«Чёрные кабинеты» . . . . .	45
Криптографы при дворе «Короля Солнце» . . . . .	46

Неизвестный криптоаналитик. . . . .	47
Чарльз Бэббидж . . . . .	49
Шифр Гронсфельда . . . . .	50

### Глава 3.

#### **История шифрования на Руси. . . . . 53**

Самое простое — использовать малоизвестный алфавит . . . . .	55
Каллиграфическая криптография . . . . .	58
Но ведь знаки для замены букв можно и придумать! . . . . .	60
«Флопяцевская азбука», «Азбука Копцева» и другие . . . . .	64
А почему бы кириллицу не заменить... кириллицей? . . . . .	71
Воспользуемся цифирью . . . . .	76
Не связать ли нам шифрочку? . . . . .	77

### Глава 4.

#### **Шифровальные машины . . . . . 81**

Алфавит точек и тире . . . . .	83
Сэмюэл Финли Бриз Морзе . . . . .	84
Невербальная связь . . . . .	85
Симфония и победа . . . . .	86
Спасите наши души. . . . .	88
Шифр Плейфера . . . . .	89
Недалеко от Парижа . . . . .	92
Машина «Энигма» . . . . .	96
Шифровки в траншеях. . . . .	100
Взлом шифра машины «Энигма» . . . . .	101
Мариан Адам Реевский . . . . .	104
Эстафету принимают англичане . . . . .	105
Истинный гений . . . . .	106
Шифры других стран . . . . .	108

Закодированные разговоры индейцев Навахо . . . . .	108
Шифр Хилла . . . . .	109
Немного линейной алгебры . . . . .	111
Шифр Хилла . . . . .	112
Криптографические протоколы . . . . .	113

## Глава 5.

### Общение при помощи нулей и единиц . . . . .115

Двоичный (бинарный) код . . . . .	117
Байты и терабайты . . . . .	118
Код ASCII . . . . .	118
Шестнадцатеричная система . . . . .	120
Системы счисления и замена основания . . . . .	123
Как измерить информацию? . . . . .	124
Гений без «Нобелевки» . . . . .	126
Ричард Уэсли Хэмминг . . . . .	129
Протокол для безопасной передачи. . . . .	130

## Глава 6.

### Кодирование в промышленных и торговых стандартах . . . . .133

Кредитные карты . . . . .	135
Алгоритм Луна . . . . .	137
Diner's Club . . . . .	139
Первые штрихкоды . . . . .	140
Норман Вудланд . . . . .	141
Штрихкод EAN-13 . . . . .	142
Применение программы EXCEL для расчёта контрольной цифры кода EAN-13 . . . . .	144
Коды QR . . . . .	145

## Глава 7.

<b>Криптография с использованием компьютера. . . . .</b>	<b>147</b>
Как безопасно распределить ключи? . . . . .	150
За алгоритмом — люди . . . . .	152
Вирусы и бэкдоры. . . . .	154
Надёжный алгоритм RSA . . . . .	155
Разумная секретность . . . . .	157
Всеобщая безопасность . . . . .	159
Удостоверение подлинности сообщений и ключей. . . . .	160
Хэш-подпись . . . . .	161
Сертификаты открытых ключей. . . . .	162
Как работает алгоритм RSA? . . . . .	164
Шифрование во вред . . . . .	166
Шифрование с помощью операции «XOR» . . . . .	167
Симметричное шифрование. . . . .	168
Асимметричное шифрование . . . . .	168
Асимметричное шифрование с одной ключевой парой . . . . .	169
Шифрование с использованием нескольких ключей. . . . .	170

## Глава 8.

<b>Квантовая криптография . . . . .</b>	<b>173</b>
Немного квантовой теории . . . . .	175
Детектирование и квант света . . . . .	176
Принцип неопределённости Гейзенберга . . . . .	176
Автор неопределённости. . . . .	177
Странная кошка. . . . .	180
Квантовые неразрушающие измерения . . . . .	182
Протоколы квантового состояния . . . . .	183

Саймон Лехна Сингх . . . . .	183
Коллапс волновой функции. . . . .	184
Невозможность клонирования . . . . .	185
Составные квантовые системы . . . . .	186
Тензорное произведение . . . . .	186
Биты и кубиты . . . . .	187
Дэвид Дойч . . . . .	188
Вычисляем квантами . . . . .	190
Нильс Хенрик Давид Бор . . . . .	190
Эрвин Рудольф Йозеф Александр Шрёдингер. . . . .	191
Передача информации по квантовым каналам. . . . .	192
Линейные коды. . . . .	193
Передача сигнальных состояний. . . . .	195
Квантовые коды коррекции ошибок . . . . .	197
Коды, исправляющие ошибку в одном кубите . . . . .	197
Усиление секретности . . . . .	199
Как избежать подслушивания. . . . .	200
Квантовые измерения . . . . .	202
Передача квантового ключа посредством перепутанных состояний . . . . .	204
Квантовая телепортация . . . . .	207
Экспериментальная реализация квантовой телепортации . . . . .	212
Стратегии подслушивателя. . . . .	215
Приём-перепосыл . . . . .	215
Критическая длина линии связи. . . . .	217
Этот шифр не одолеть . . . . .	219
Послание из Вавилона. . . . .	221
От сантиметров к километрам абсолютной секретности . . . . .	225

## Глава 9.

245

### И, наконец, что же это — квантовый компьютер? . . . . . 227

Возможность создания  
квантового компьютера . . . . . 230

Устройство квантового компьютера . . . . . 231

Квантовый бит . . . . . 232

Квантовый регистр . . . . . 233

Квантовые компьютеры сегодня . . . . . 235

Взгляд в будущее . . . . . 236