ŋqqdɣeɎ bɆ dəqɆbɎəe d ɐɔɐɓɔɎ ɟqqdɎqɏè

Виктор де Касто

СЕРИЯ ПРОСТО

ПРО КРИПТОГРАФИЮ

Автор идеи
и научный редактор серии
СЕРГЕЙ ДЕМЕНОК

НАУЧНО-ПОПУЛЯРНОЕ
ИЗДАТЕЛЬСТВО
«СТРАТА»
Санкт-Петербург.2020

ŋqqdɣeɎ bɆ dəqɆbɎəe d ɐɔɐɓɔɎ ɟqqdɎqɏè

УДК 001, 501, 510
ББК 22.1
К 28

К 28 ПРО КРИПТОГРАФИЮ (Символ — машина — квант) — СПб.: Страта, 2020. — 240 с., с илл. — (серия «Просто»)

ISBN 978-5-907314-15-3

Чем больше одни стремятся что-то скрыть, тем больше другие хотят это «что-то» узнать. Когда люди только научились писать, их тайны материализовались, представ в образе символов, иероглифов, букв, цифр. Но в таком виде они стали доступны другим. С этого времени началось извечное соревнование между шифровальщиками, пытающимися скрыть информацию, и криптоаналитиками, стремящимися расшифровать ее.

Криптография сегодня — это область научных, прикладных, инженерно-технических исследований, основанная на фундаментальных понятиях математики, физики, теории информации и сложности вычислений.

В книге рассказывается об истории криптографии: от примитивных систем шифрования и дешифровки, придуманных людьми еще в древние времена, до современных компьютерных алгоритмов — как существующих, так и тех, над которыми работают нынешние ученые-криптографы.

Книга предназначена для широкого круга читателей.

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 978-5-907314-15-3

© Деменок С. Л., текст, 2020
© ООО «Страта», 2020

СОДЕРЖАНИЕ

ŋqdpɏeɎ þɆ dedɆþɎɜe d ɕɜɑbɕɏ ɟqddɎqɏè

ŋqdpɏeɎ þɆ dedɆþɎɜe d ɕɜɑbɕɏ ɟqddɎqɏè

ŋqdpʮeɐ⅄ bɆ dəbɆbʮɜə d ɕɔɑbɔʮ Ɉqdqʮqʮè

ŋqdpʮeɐ⅄ bɆ dəbɆbʮɜə d ɕɔɑbɔʮ Ɉqdqʮqʮè

ŋqdqɏeɎ bɆ dəqƐbɎзə b ɕɑɑбɔɏ ɈqdqɎqɏè

ŋqdqɏeɎ bɆ dəqƐbɎзə b ɕɑɑбɔɏ ɈqdqɎqɏè