ŋqdqɏeɏ bɇ dəqɇbɏɜə d ɕɑɑbɕɏ ɟqqdɎqɏè

УДК 004.382
ББК 32.973-018
O57

Омассон Ж.-Ф.

O57 О криптографии всерьез / пер. с англ. А. А. Слинкина. – М.: ДМК Пресс, 2022. – 328 с.: ил.

ISBN 978-5-97060-975-0

В этом практическом руководстве по современному шифрованию анализируются фундаментальные математические идеи, лежащие в основе криптографии. Рассказывается о шифровании с аутентификацией, безопасной случайности, функциях хеширования, блочных шифрах и методах криптографии с открытым ключом, в частности RSA и криптографии на эллиптических кривых. Вы узнаете о том, как выбирать наилучший алгоритм или протокол, как избежать типичных ошибок безопасности и как задавать правильные вопросы поставщику. В заключительной части книги рассматриваются темы повышенной сложности, например TLS, а также обсуждается будущее криптографии в эпоху квантовых компьютеров.

В каждой главе приводятся примеры работы алгоритмов и материалы для дополнительного изучения.

Издание будет полезно как профессиональным разработчикам, так и тем, кто хочет разобраться в основах современной криптографии и успешно применять методы шифрования.

УДК 004.382
ББК 32.973-018

Title of English-language original: Serious Cryptography: A Practical Introduction to Modern Encryption, ISBN 9781593278267, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2021 by DMK Press Publishing under license by No Starch Press Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-59327-826-7 (англ.)
ISBN 978-5-97060-975-0 (рус.)

© Jean-Philippe Aumasson, 2018
© Перевод, оформление, издание, ДМК Пресс, 2021

ŋqdqɏeɏ bɇ dəqɇbɏɜə d ɕɑɑbɕɏ ɟqqdɎqɏè

СОДЕРЖАНИЕ

ŋqdpɏeɏ bɆ dedɆbɏɜe d ɕɑɑbɔɏ Ɉqdpɏqɏè

ŋqdpɏeɏ bɆ dedɆbɏɜe d ɕɑɑbɔɏ Ɉqdpɏqɏè

ђqdqʎeʎ bɆ dədɆbʎɜə d ɛɔɑbɔʎ Ɉqdqʎqʎè

ђqdqʎeʎ bɆ dədɆbʎɜə d ɛɔɑbɔʎ Ɉqdqʎqʎè

ђqdpҷеɏ bɆ dәdɆbӰзә d ɕoɑpɕҷ Ɉqddүqҷѐ

ђqdpҷеɏ bɆ dәdɆbӰзә d ɕoɑpɕҷ Ɉqddүqҷѐ

ŋqdqyeY bE dedEbYse d eoaboY Jqddyqyè

ŋqdqyeY bE dedEbYse d eoaboY Jqddyqyè