Рябко Б. Я.
Фионов А. Н.

ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

Горячая линия–Телеком

2 издание

Б. Я. Рябко, А. Н. Фионов

ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

2 издание

Москва
Горячая линия - Телеком
2013

УДК 621.391
ББК 32.801.4
Р98

Рябко Б. Я., Фионов А. Н.

Р98 Основы современной криптографии и стеганографии. – 2-е изд. – М.: Горячая линия – Телеком, 2013. – 232 с.: ил.

ISBN 978-5-9912-0350-0.

В монографии изложены основные подходы и методы современной криптографии и стеганографии для решения задач, возникающих при обработке, хранении и передаче информации. Рассмотрены основные шифры с открытыми ключами, методы цифровой подписи, основные криптографические протоколы, блоковые и потоковые шифры, криптографические хеш-функции, а также редко встречающиеся в литературе вопросы о конструкции доказуемо невскрываемых криптосистем и криптографии на эллиптических кривых. Рассмотрены вопросы, связанные с использованием случайных и псевдослучайных чисел в системах защиты информации. Приведено описание основных идей и методов современной стеганографии. Подробно описаны алгоритмы, лежащие в основе криптографических отечественных и международных стандартов. Многие из приведенных в книге результатов исследований, полученных авторами в последние годы, признаны специалистами в России и за рубежом.

Для исследователей и специалистов, работающих в области защиты информации, будет полезна для аспирантов и студентов.

ББК 32.801.4

Адрес издательства в Интернет www.techbook.ru

Научное издание

Рябко Борис Яковлевич
Фионов Андрей Николаевич

Основы современной криптографии и стеганографии

Монография

2-е издание

Подписано к печати 15.06.2013. Формат 60×88 1/16. Усл. печ. л. 14,5. Изд. № 130350.
Тираж 300 экз. (1-й завод 100 экз.)

ISBN 978-5-9912-0350-0

ОГЛАВЛЕНИЕ