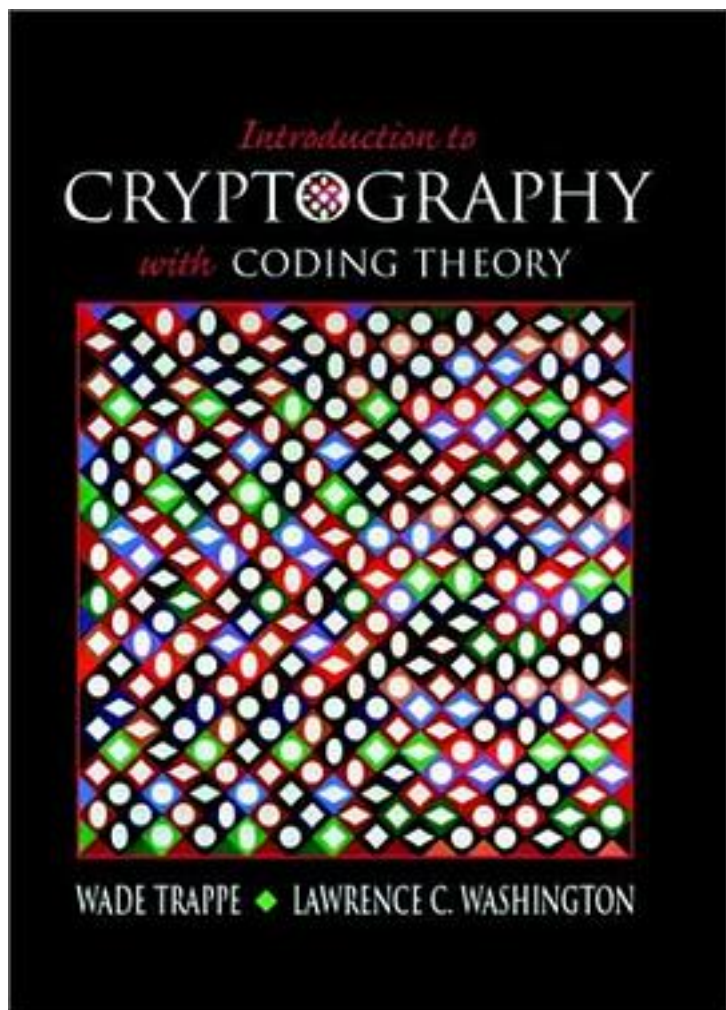# Introduction to Cryptography with Coding Theory

[Introduction to Cryptography with Coding Theory_下载链接1_](#)

著者:Wade Trappe

出版者:Pearson

出版时间:2005-7-25

装帧:Hardcover

isbn:9780131862395

With its conversational tone and practical focus, this text mixes applied and theoretical

aspects for a solid introduction to cryptography and security, including the latest significant advancements in the field. Assumes a minimal background. The level of math sophistication is equivalent to a course in linear algebra. Presents applications and protocols where cryptographic primitives are used in practice, such as SET and SSL. Provides a detailed explanation of AES, which has replaced Feistel-based ciphers (DES) as the standard block cipher algorithm. Includes expanded discussions of block ciphers, hash functions, and multicollisions, plus additional attacks on RSA to make readers aware of the strengths and shortcomings of this popular scheme. For engineers interested in learning more about cryptography.

作者介绍:

目录:

标签

Cryptography

密码学

Textbook

pqc

ebook

Math

English

Computer

评论

初学者友好

I've had to get out of bed to finish reading this one. The fluidity of number theory applications made me horny as hell.

Introduction to Cryptography with Coding Theory_下载链接1_

书评

from china pub 2第1章 密码学及其应用概述 1.1 安全通信 1.1.1 可能的攻击 1.1.2 对称和公钥算法 1.1.3 密钥长度 1.2 密码学应用 第2章 传统密码系统 2.1 移位密码 2.2 仿射密码 2.3 维吉内尔密码 2.3.1 算出密钥长...

Introduction to Cryptography with Coding Theory_下载链接1_