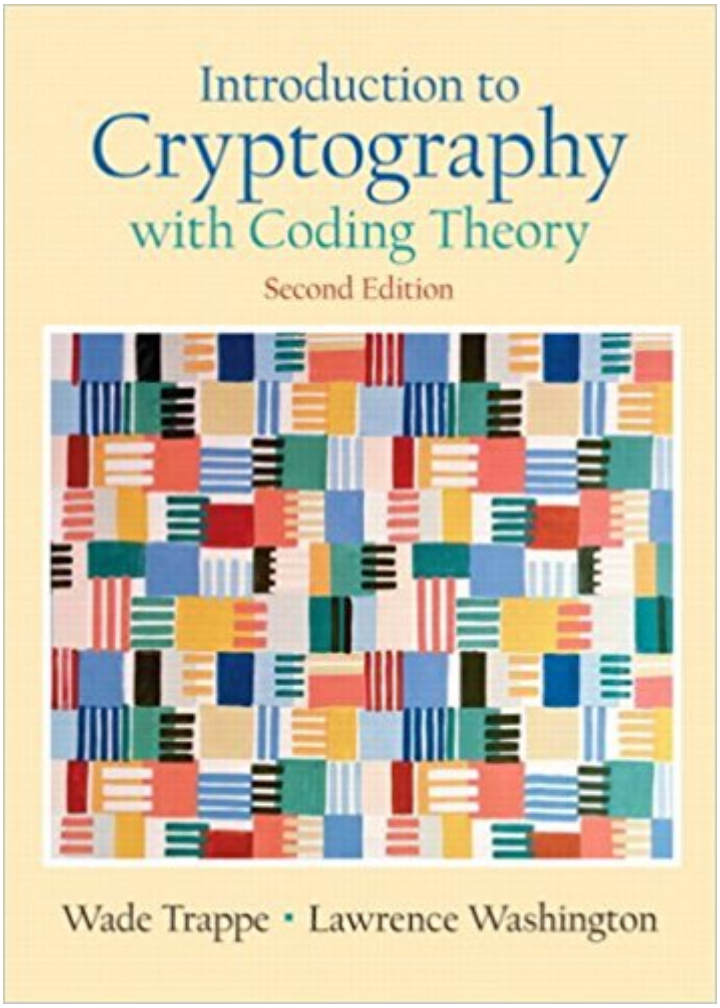
Introduction To Cryptography With Coding Theory (2nd Edition)



Synopsis

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.

Book Information

Hardcover: 592 pages
Publisher: Pearson; 2 edition (July 25, 2005)
Language: English
ISBN-10: 0131862391
ISBN-13: 978-0131862395
Product Dimensions: 7.2 x 1.4 x 9.4 inches
Shipping Weight: 2.2 pounds (View shipping rates and policies)
Average Customer Review: 3.9 out of 5 starsÂ Â See all reviewsÂ (18 customer reviews)
Best Sellers Rank: #152,285 in Books (See Top 100 in Books) #2 inÂ Books > Computers & Technology > Programming > Software Design, Testing & Engineering > Coding Theory #39 inÂ Books > Computers & Technology > Security & Encryption > Cryptography #157 inÂ Books > Textbooks > Computer Science > Networking

Customer Reviews

The book presents modern cryptography in a way that anyone can understand and makes even the most difficult of subjects easy to learn. It does present in depth math analysis of various ciphers, so read it thoroughly is a must!

This an excellant reference text-book for cryptography students and teachers, and could be by far the most comprehensive introductory level cryptography text-book. A welcome addition for every math/computer-science major’s personal library.Nema

This book may be a good reference--maybe--, but there tends to be a lot of glossing over, with core concepts of complex things being left unexplained. They’re probably obvious to someone more versed in the field, but for an "Introduction" book I’d hope for a bit more.On the other hand, certain parts of this book were quite solid. Just don’t expect to use it as your only reference.

Hi. This is a very good book for university studies or also for personal use too. Easy to read and understand. There are few mathematical details (this is a negative feature) but it explains very well all arguments. The only really negative thing is the cost, a little much ...Otherwise, i suggest you this book.

Trappe and Washington give us a very up to date education in cryptography, circa 2005. The discourse is for a sophisticated maths student who, however, need never have encountered cryptography before. The level of mathematical treatment is good and rigourous. With theorems stated and proved at a level that should satisfy even a picky mathematician.The recent nature of the book is reflected in several places. Notably where it explains the Advanced Encryption Standard, or Rijndael. This is significant because it is endorsed by the US National Institute of Standards and Technology as the replacement for DES, in such contexts as electronic commerce. (DES is also covered by the book.)Interestingly, the authors offer a short chapter on digital cash. A fascinating look at a possible future direction of a (physically) cashless society. Other texts on cryptography rarely cover the topic, so it’s good to see it here. Yes, the first implementations of digital cash largely died in the dot com crash. But the idea lives on, and may yet take fruit. It has solid intellectual foundations, as shown by the book.Then there is an even more speculative chapter on quantum cryptography. Radically different from the symmetric and public key cryptosystems described in the rest of the book. Who knows how quantum cryptography will turn out? Some very hard physical problems need to be solved.

I’ve read (or skimmed, as the case may be) some other writings on cryptography and none of them are really as clear as Trappe and Washington’s book. Applied Cryptography comes somewhat close, but doesn’t include enough math. Intro. to Cryptography with Coding Theory comes as close to the right balance between math and cryptography as possible. Right now, I’m taking one of Prof. Trappe’s classes and I always am confident that if I feel I’m not going to remember the part of the lecture, I can easily refer to the book. The book is actually good enough to discourage me from taking notes and just pay attention instead. Not only that, but the code that’s provided is offered in

Maple, MATLAB, and Mathematica. Could you ask for more?

Knowing very little about cryptography when I started, I found this book taught me the fundamentals of cryptography with useful examples as it walked me through the material. In addition, it was a useful reference for applying this newfound knowledge to the actual practice in use today, especically on the internet. This book is a must-have for anyone needing an understanding of cryptography.

If more mathematics textbooks were written like this one, the number of mathematicians/scientists in the world would be much greater.The book is an absolute pleasure to read. The discoursive style makes what surely can be considered as a hard subject smooth and easily flowing.The subject is very well covered and the structure of the book is just fine, even for self-study.Algorithms, encryption methods, mathematical theorems are nicely and elegantly explained and no previous knowledge is necessary in any of the fields.At the end of many explanations or proofs I found myself stunned by the brevity and beauty of the argument.I enjoyed also the nice software support and exercise coming with the books.

Developers, Coding, CSS, PHP Book 2) Cryptography and Network Security: Principles and Practice (7th Edition) Cryptography and Network Security: Principles and Practice (6th Edition) Selected Unsolved Problems in Coding Theory (Applied and Numerical Harmonic Analysis) Key Papers in the Development of Coding Theory (Ieee Press Selected Reprint Series) A Student's Guide to Coding and Information Theory Understanding Cryptography: A Textbook for Students and Practitioners Cryptography Engineering: Design Principles and Practical Applications Cryptography InfoSec Pro Guide (Beginner's Guide) Circuit Engineering & Cryptography & Hacking Cryptography and Network Security: Principles and Practice