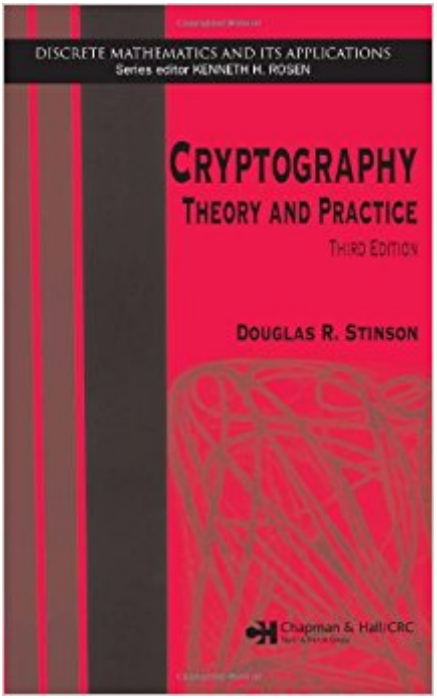
Cryptography: Theory And Practice, Third Edition (Discrete Mathematics And Its Applications)



Synopsis

THE LEGACYÃ¢â ¬Â|First introduced in 1995, Cryptography: Theory and Practice garnered enormous praise and popularity, and soon became the standard textbook for cryptography courses around the world. The second edition was equally embraced, and enjoys status as a perennial bestseller. Now in its third edition, this authoritative text continues to provide a solid foundation for future breakthroughs in cryptography.WHY A THIRD EDITION?The art and science of cryptography has been evolving for thousands of years. Now, with unprecedented amounts of information circling the globe, we must be prepared to face new threats and employ new encryption schemes on an ongoing basis. This edition updates relevant chapters with the latest advances and includes seven additional chapters covering:Pseudorandom bit generation in cryptographyEntity authentication, including schemes built from primitives and special purpose "zero-knowledge" schemesKey establishment including key distribution and protocols for key agreement, both with a greater emphasis on security models and proofsPublic key infrastructure, including identity-based cryptographySecret sharing schemesMulticast security, including broadcast encryption and copyright protectionTHE RESULTÃ¢â ¬Â|Providing mathematical background in a "just-in-time" fashion, informal descriptions of cryptosystems along with more precise pseudocode, and a host of numerical examples and exercises, Cryptography: Theory and Practice, Third Edition offers comprehensive, in-depth treatment of the methods and protocols that are vital to safeguarding the mind-boggling amount of information circulating around the world.

Book Information

Series: Discrete Mathematics and Its Applications (Book 30)
Hardcover: 616 pages
Publisher: Chapman and Hall/CRC; 3 edition (November 1, 2005)
Language: English
ISBN-10: 1584885084
ISBN-13: 978-1584885085
Product Dimensions: 6.3 x 1.4 x 9.6 inches
Shipping Weight: 1.5 pounds (View shipping rates and policies)
Average Customer Review: 4.0 out of 5 stars 26 customer reviews
Best Sellers Rank: #276,994 in Books (See Top 100 in Books) #45 inÃ Â Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #81 inÃ Â Books > Computers & Technology > Security & Encryption > Encryption #84 inÃ Â Books > Computers & Technology > Security &

Encryption > Cryptography

Customer Reviews

Douglas R. Stinson’s Cryptography: Theory and Practice is a mathematically intensive examination of cryptography, including ciphers, the Data Encryption Standard (DES), public key cryptography, one-way hash functions, and digital signatures. Stinson’s explication of "zero-sum proofs"--a process by which one person lets another person know that he or she has a password without actually revealing any information--is especially good. If you are new to the math behind cryptography but want to tackle it, the author covers all of the required background to understand the real mathematics here. Cryptography includes extensive exercises with each chapter and makes an ideal introduction for any math-literate person willing to get acquainted with this material. --This text refers to an out of print or unavailable edition of this title.

"It is by far the most suitable text for undergraduate and graduate courses on the subject in mathematics and computer science departments. Besides having breadth and scope in the choice of topics, many of them are dealt with in much more depth than what can be found elsewhere at this level . . . If you really want to learn some cryptography this is probably the best available text." Ã¢â ¬â œ Peter Shiu, Department of Mathematical Sciences, Loughborough University, in The Mathematical Gazette, March 2007 ". . . the book is very well suited for a course in crypotography." Ã¢â ¬â œ Bran van Asch, in Mathematical Reviews, 2007f

This was a book for school so I don’t have much to say about it. I think it explained things pretty well. I really enjoyed this course, but I for sure did not read the whole thing. As for the seller, book did not have any problems, came in good condition.

Purchased this for a class and found it very interesting and helpful. I got a lot out of this textbook and I recommend it for anyone looking to leran more on the subject.

The textbook introduces various areas of cryptography to undergraduate and graduate students in mathematics and computer science. It covers classical cryptosystems, Shannon’s approach to perfect secrecy, block ciphers and hash functions. Public-key cryptography, signature schemes and pseudo random number generators are also discussed in detail. Other chapters discuss key distribution and entity authentication. The book is geared toward serving as a class-room textbook

with numerous solved examples and exercises. It genuinely deserves its reputation as an indispensable textbook for cryptography teaching.

I bought it for a school class and now I use it as reference material for work. It is one of the few books that survived the cut for me.

I found the problems in this book were sometimes hard to follow. It sometimes makes assumptions that the step that follows is obvious.

As other people have pointed out, this is not a mathematics book, and it is not an algorithm (recipies) book. It could be a great book for people that are interested in learning these tools to actually use them, either in a research or product development context (something besides homework). Unfortunately, the number of typos, in key mathematical expressions AND PORTIONS OF THE EXPLANATIONS is staggering. Go to the author's web page and you will find that some chapters, like 4 for example, average more than one typo per page (and some of these 'typos' are full sentences, or math expressions that do not look like anything that is actually printed on the page). If you do not have that errata sheet handy, you will waste a lot of time trying to understand the text, or trying to solve the exercises. If you are trying to learn from this book, without attending a class and without the errata, you will simply give up. It is a real shame because it has all the makings of a great book.

This textbook strikes a good balance between mathematics and explanation. The topics are organized in a clear and concise manner and the exercises test the concepts well.

I am a Cybersecurity student at SEMO and am using this as a reference book. Excellent condition when advertised as "very good". This is the textbook for one of my Spr13 classes.

29th Edition (Discrete Mathematics and Its Applications) Discrete Mathematics and Its Applications Seventh Edition (Higher Math) Student's Solutions Guide to Accompany Discrete Mathematics and Its Applications, 7th Edition Introduction to Mathematical Logic, Sixth Edition (Discrete Mathematics and Its Applications) Introduction to Mathematical Logic, Fourth Edition (Discrete Mathematics and Its Applications) Discrete Mathematics and Applications, Second Edition (Textbooks in Mathematics) Discrete Mathematics and Its Applications (Higher Math) Discrete Mathematics and Its Applications Discrete Mathematics with Graph Theory (Classic Version) (3rd Edition) (Pearson Modern Classics for Advanced Mathematics Series) A Course in Number Theory and Cryptography (Graduate Texts in Mathematics) Third Eye: Third Eye Activation Mastery, Easy And Simple Guide To Activating Your Third Eye Within 24 Hours (Third Eye Awakening, Pineal Gland Activation, Opening the Third Eye) Discrete and Combinatorial Mathematics (Classic Version) (5th Edition) (Pearson Modern Classics for Advanced Mathematics Series) Discrete Algorithmic Mathematics, Third Edition Schaum's Outline of Discrete Mathematics, Revised Third Edition (Schaum's Outlines) Discrete Mathematics with Graph Theory, 3rd Edition Discrete Mathematics with Graph Theory International Edition