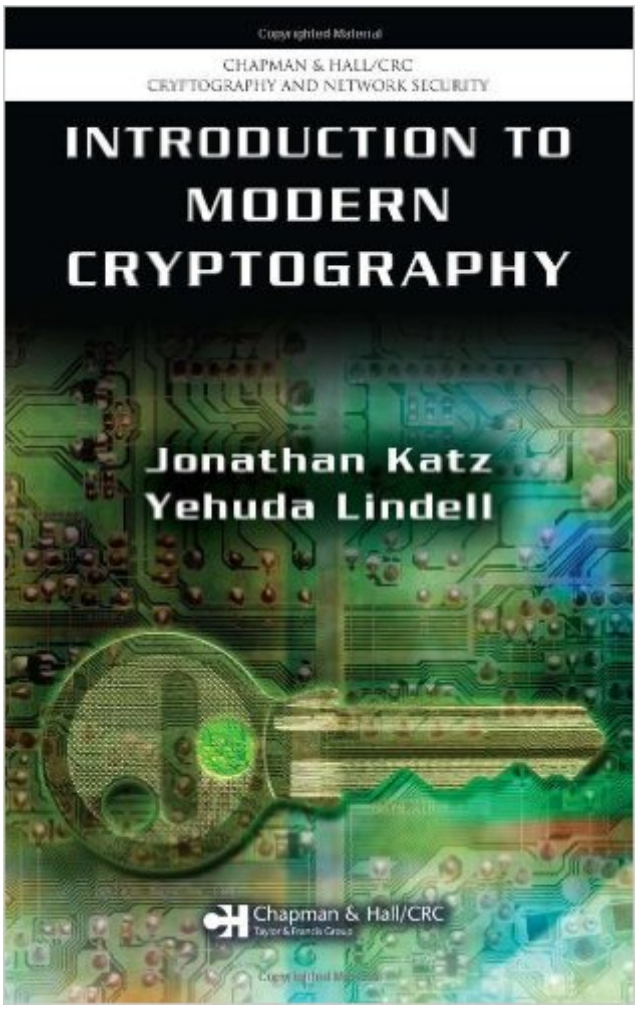
Introduction To Modern Cryptography: Principles And Protocols (Chapman & Hall/CRC Cryptography And Network Security Series)



Synopsis

Cryptography plays a key role in ensuring the privacy and integrity of data and the security of computer networks. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of modern cryptography, with a focus on formal definitions, precise assumptions, and rigorous proofs.The authors introduce the core principles of modern cryptography, including the modern, computational approach to security that overcomes the limitations of perfect secrecy. An extensive treatment of private-key encryption and message authentication follows. The authors also illustrate design principles for block ciphers, such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and present provably secure constructions of block ciphers from lower-level primitives. The second half of the book focuses on public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, El Gamal, and other cryptosystems. After exploring public-key encryption and digital signatures, the book concludes with a discussion of the random oracle model and its applications.Serving as a textbook, a reference, or for self-study, Introduction to Modern Cryptography presents the necessary tools to fully understand this fascinating subject.

Book Information

Series: Chapman & Hall/CRC Cryptography and Network Security Series
Hardcover: 552 pages
Publisher: Chapman and Hall/CRC; 1 edition (August 31, 2007)
Language: English
ISBN-10: 1584885513
ISBN-13: 978-1584885511
Product Dimensions: 9.5 x 6.5 x 1.3 inches
Shipping Weight: 2 pounds
Average Customer Review: 4.5 out of 5 starsÂ Â See all reviewsÂ (11 customer reviews)
Best Sellers Rank: #279,963 in Books (See Top 100 in Books) #40 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #70 inÂ Books > Computers & Technology > Certification > CompTIA #264 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

I used this book for a course on modern cryptography held by Prof. Persiano of the University of Salerno, Italy.I read, consulted, and studied other books about cryptography, but 'INTRODUCTION

TO MODERN CRYPTOGRAPHY' by Katz and Lindell is in my humble opinion THE BEST.The book has a theoretical flavor, it is mathematically rigorous, but it is very readable and fluent, and presents the motivating discussions beneath each topic.The book is fully self-contained, and gives the necessary background for each topic (for example there is a lot of basic computational number theory necessary for introducing the topic of 'public key').The beauty of the book is in that the authors don't present a collection of protocols, with no links each other, but the flow is sequential and motivated (in contrast to books which present topics only for filling the pages).All the theorems are proved and the treatment is rigorous, but the theory is developed from scratch, and the book is oriented to beginner students, though it presents also advanced stuff and is one of the most advanced book for beginners.The main contents of the book are:1) Perfect security and Shannon's theorem (information theoretic security)2) Computational security, indistinguishability, CPA3) Pseudorandomness4) One-way functions, hard-core predicate, Levin's theorem5) Message Authentication Codes6) Costructions of Pseudorandom objects, AES, Substitution-Permutation networks7) Relation between Private-Key, one-way functions and pseudrandomness.

It was very nice to see how security would be possibly defined in a sense different from (and more relaxed than) information-theoretic secrecy. It was nice to see how different definitions would lead to different levels of security, or in other words, each definition gives a guarantee of security against a certain class of real-life security threats (or attacks) and takes also into account very practical issues like dealing with computationally bounded adversaries. Moreover, introducing the notion of security using those definitions made the whole setting, not only mathematically rigorous, but also coherent, structured, and well-founded, without losing contact with practical concerns and real-life scenarios. Even more, this setting gave a neat and mathematically sound way to attain a proven notion of security rather than just introducing or suggesting schemes that show "good" performance in practice without being able to say anything, or quantify the security they provide on a more fundamental level. Another thing I also liked very much and is related to the point above, is how the book moves on to the point where it was shown that the provable security of almost (if not all) the encryption schemes (either private-key or public-key based) as well as authentication codes and signature schemes is based on the corner stone assumption of existence of one-way functions (one-way permutations). It was very elegant the way a one-way function (permutation) was defined and the way it is used to prove security in one sense or the other. It fits in very well in the development of the theory and made the whole structure very homogeneous.

Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/CRC Cryptography and Network Security Series) Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) Introduction to Network Security (Chapman & Hall/CRC Computer and Information Science Series) Applied Cryptography: Protocols, Algorithms, and Source Code in C [APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C BY Schneier, Bruce (Author) Nov-01-1995 Coding Theory and Cryptography: The Essentials, Second Edition (Chapman & Hall/CRC Pure and Applied Mathematics) Web 2.0 and Beyond: Principles and Technologies (Chapman & Hall/CRC Textbooks in Computing) An Introduction to Multicomplex SPates and Functions (Chapman & Hall/CRC Pure and Applied Mathematics) Algorithms in Bioinformatics: A Practical Introduction (Chapman & Hall/CRC Mathematical and Computational Biology) Introduction to Computational Biology: Maps, Sequences and Genomes (Chapman & Hall/CRC Interdisciplinary Statistics) Introduction to Probability (Chapman & Hall/CRC Texts in Statistical Science) Stochastic Processes: An Introduction, Second Edition (Chapman & Hall/CRC Texts in Statistical Science) An Introduction to Partial Differential Equations with MATLAB (Chapman & Hall/CRC Applied Mathematics & Nonlinear Science) A Concise Introduction to Pure Mathematics, Fourth Edition (Chapman Hall/CRC Mathematics) Home Security: Top 10 Home Security Strategies to Protect Your House and Family Against Criminals and Break-ins (home security monitor, home security system diy, secure home network) Image Processing and Acquisition using Python (Chapman & Hall/CRC Mathematical and Computational Imaging Sciences Series) Data Classification: Algorithms and Applications (Chapman & Hall/CRC Data Mining and Knowledge Discovery Series) Numerical Techniques for Direct and Large-Eddy Simulations (Chapman & Hall/CRC Numerical Analysis and Scientific Computing Series) The Garbage Collection Handbook: The Art of Automatic Memory Management (Chapman & Hall/CRC Applied Algorithms and Data Structures series) Computational Methods of Feature Selection (Chapman & Hall/CRC Data Mining and Knowledge Discovery Series) Bayesian Designs for Phase I-II Clinical Trials (Chapman & Hall/CRC Biostatistics Series)