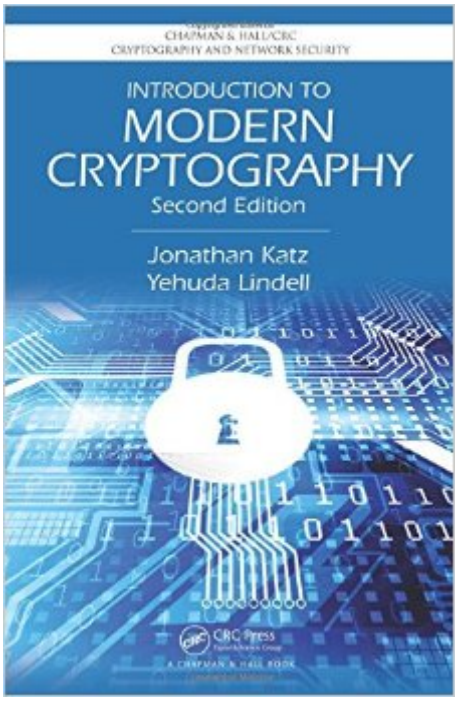
Introduction To Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography And Network Security Series)



Synopsis

Cryptography is ubiquitous and plays a key role in ensuring data secrecy and integrity as well as in securing computer systems more broadly. Introduction to Modern Cryptography provides a rigorous yet accessible treatment of this fascinating subject. The authors introduce the core principles of modern cryptography, with an emphasis on formal definitions, clear assumptions, and rigorous proofs of security. The book begins by focusing on private-key cryptography, including an extensive treatment of private-key encryption, message authentication codes, and hash functions. The authors also present design principles for widely used stream ciphers and block ciphers including RC4, DES, and AES, plus provide provable constructions of stream ciphers and block ciphers from lower-level primitives. The second half of the book covers public-key cryptography, beginning with a self-contained introduction to the number theory needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems (and others), followed by a thorough treatment of several standardized public-key encryption and digital signature schemes. Integrating a more practical perspective without sacrificing rigor, this widely anticipated Second Edition offers improved treatment of: Stream ciphers and block ciphers, including modes of operation and design principles Authenticated encryption and secure communication sessions Hash functions, including hash-function applications and design principles Attacks on poorly implemented cryptography, including attacks on chained-CBC encryption, padding-oracle attacks, and timing attacks The random-oracle model and its application to several standardized, widely used public-key encryption and signature schemes Elliptic-curve cryptography and associated standards such as DSA/ECDSA and DHIES/ECIES Containing updated exercises and worked examples, Introduction to Modern Cryptography, Second Edition can serve as a textbook for undergraduate- or graduate-level courses in cryptography, a valuable reference for researchers and practitioners, or a general introduction suitable for self-study.

Book Information

Series: Chapman & Hall/CRC Cryptography and Network Security Series
Hardcover: 603 pages
Publisher: Chapman and Hall/CRC; 2 edition (November 6, 2014)
Language: English
ISBN-10: 1466570261
ISBN-13: 978-1466570269
Product Dimensions: 1.2 x 6.2 x 9.2 inches
Shipping Weight: 2.2 pounds

Average Customer Review: 3.7 out of 5 starsÂ Â See all reviewsÂ (7 customer reviews)
Best Sellers Rank: #40,903 in Books (See Top 100 in Books) #4 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #14 inÂ Books > Computers & Technology > Security & Encryption > Encryption #16 inÂ Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

I have not finished the book yet, but from material I went so far and from Jonathan Katz's course on Cryptography I think I can describe authors way of providing information. I would characterize it in two keywords: rigorous and complete. Other materials I have met were maybe more lively but this one is is the best if you are really serious about crypto. It will give all the details you need to understand and work with modern cryptographic primitives. I will teach how to prove or disprove properties of various cryptographic schemes.

A rigorous treatment based on clear assumptions and proofs derived from those assumptions. Mastering the topic is not easy, but Katz's writing is clear.

I think this is simply the very best introductory book available. It does require some math background, but nothing extensive. Anyone with a basic computer science education should be able to follow along. To many books are either at too complex a level, or overly simple. I think this book nailed it.

Great Intro to modern cryptography

& Hall/CRC Texts in Statistical Science) A Concise Introduction to Pure Mathematics, Fourth Edition (Chapman Hall/CRC Mathematics) 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) An Introduction to Partial Differential Equations with MATLAB (Chapman & Hall/CRC Applied Mathematics & Nonlinear Science) 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)