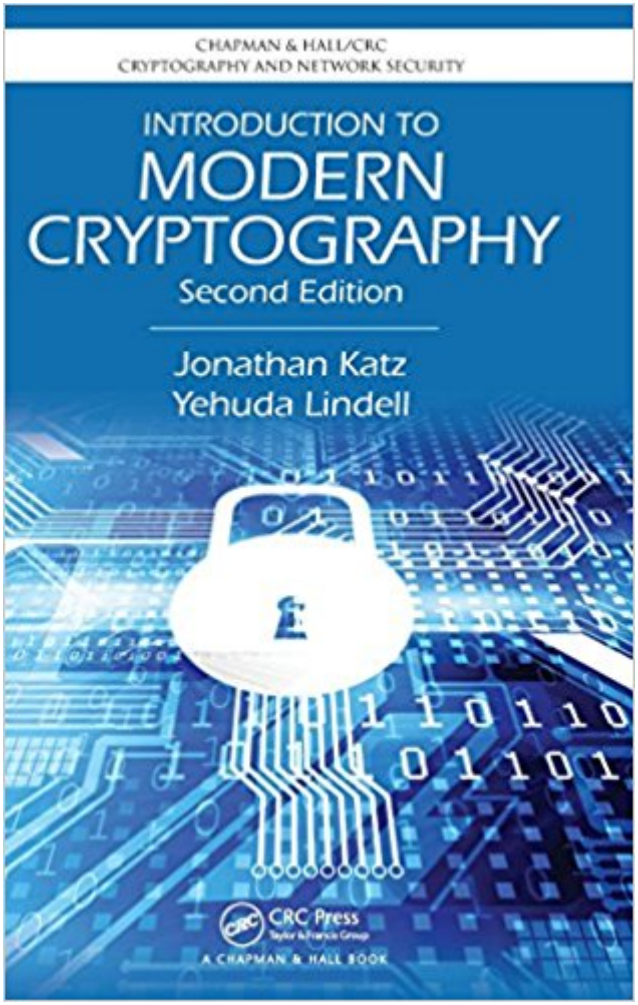
Introduction To Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography And Network Security Series)



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: 6.1 x 1.3 x 9.2 inches
Shipping Weight: 2.2 pounds (View shipping rates and policies)

Average Customer Review: 3.9 out of 5 stars 13 customer reviews

Best Sellers Rank: #21,378 in Books (See Top 100 in Books) #4 inÃ Â Books > Science & Math > Mathematics > Pure Mathematics > Combinatorics #10 inÃ Â Books > Computers & Technology > Security & Encryption > Cryptography #10 inÃ Â Books > Computers & Technology > Security & Encryption > Encryption

Customer Reviews

"The work is comprehensive, rigorous, and yet accessible for dedicated students."Ã¢â ¬â ¢Computing Reviews, October 2015 "Ã¢â ¬Â| this book fills a significant gap among previous cryptography textbooks by explicitly discussing the philosophy behind this approach, gradually building up the relevant theory and giving a broad overview of the discipline conceived within this framework. The result is a coherent picture of the field that provides a pleasing clarity in its explanation of this perspective through a systematic, step-by-step development of important concepts. Ã¢â ¬Â| The material from the first edition has been restructured and expanded, with an emphasis on practical aspects that provides a nice counterpoint to the theory and helps to highlight its real-world relevance. Ã¢â ¬Â| This textbook is appropriate for use in teaching at either an advanced undergraduate or graduate level Ã¢â ¬Â| a particularly valuable resource for graduate students with a computer science or mathematics background who are seeking a pathway to understanding the current cryptography research literature. In the preface, the authors mention their aim of treating modern cryptography through a unified approach that is rigorous yet accessibleÃ¢â ¬â ¢Introduction to Modern Cryptography achieves this admirably."Ã¢â ¬â ¢Mathematical Reviews, August 2015 Praise for the First Edition:"This book is a comprehensive, rigorous introduction to what the authors name Ã¢â ¬Ëœmodernâ ¬â„¢ cryptography. Ã¢â ¬Â| a novel approach to how cryptography is taught, replacing the older, construction-based approach. Ã¢â ¬Â| The concepts are clearly stated, both in an intuitive fashion and formally. Ã¢â ¬Â| I would heartily recommend this book to anyone who is interested in cryptography. Ã¢â ¬Â| The exercises are challenging and interesting, and can benefit readers of all academic levels."Ã¢â ¬â ¢IACR Book Reviews, January 2010 "Over the past 30 years, cryptography has been transformed from a mysterious art into a mathematically rigorous science. The textbook by Jonathan Katz and Yehuda Lindell finally makes this modern approach to cryptography accessible to a broad audience. Readers of this text will learn how to think precisely about the security of protocols against arbitrary attacks, a skill that will remain relevant and useful regardless of how technology and cryptography standards change. The book uses just enough

formalism to maintain precision and rigor without obscuring the development of ideas. It manages to convey both the theory’s conceptual beauty and its relevance to practice. I plan to use it every time I teach an undergraduate course in cryptography."Ã¢â ¬â ¢Salil Vadhan, Harvard University, Cambridge, Massachusetts, USA "The greatest attribute is the fact that the material is presented in such a unified way. This is not just a collection of topics from cryptography thrown together at random. One topic leads effortlessly to the next. As such, this is a virtually indispensable resource for modern cryptography."Ã¢â ¬â ¢Donald L. Vestal, South Dakota State University, Brookings, USA, MAA Online, July 2008 "Ã¢â ¬Â¦ an excellent introduction to the theoretical background of cryptography. It would be a fine textbook for an advanced undergraduate (or graduate) course in theoretical computer science for students who have already seen the rudiments of cryptography. It will be a valuable reference for researchers in the field."Ã¢â ¬â ¢Steven D. Galbraith, Mathematical Reviews, 2009 "The book is highly recommended as a textbook in cryptography courses at graduate or advanced undergraduate levels. Ã¢â ¬Â¦ covers, in a splendid way, the main notions of current cryptography from the point of view of information-theoretical security. This corresponds indeed to a modern cryptography approach."Ã¢â ¬â ¢Guillermo Morales-Luna, Zentralblatt MATH, Vol. 1143

Jonathan Katz is a professor of computer science at the University of Maryland, and director of the Maryland Cybersecurity Center. He has published over 100 articles on cryptography, and serves as an editor of the Journal of Cryptology, the premier journal of the field. Prof. Katz has been invited to give introductory lectures on cryptography for audiences in academia, industry, and government, as well as an on-line cryptography course through Coursera. Yehuda Lindell is a professor of computer science at Bar-Ilan University. He has published more than 90 articles on cryptography and four books, and has considerable industry experience in deploying cryptographic schemes. Professor Lindell lectures widely in both academic and industry venues on both theoretical and applied cryptography, and has been recognized with two prestigious grants from the European Research Council.

This is a serious introduction book. I enjoyed Katz’s course on Coursera.Note this is theoretical. If you are looking for material on hardware or physical attacks like side channel attacks or fault injection attacks, you will need to look elsewhere. With that said, it is useful as a reference even after you have digested the material because Katz is very particular with rigor, notation, and word choice -- the result of a mathematician who cares about communication.

Awesome book on a tough subject.

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.

well written book

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.

Very detailed and well-written text.

Great book!

Great Intro to modern cryptography

(Chapman & Hall/CRC The R Series) Modeling and Analysis of Stochastic Systems, Second Edition (Chapman & Hall/CRC Texts in Statistical Science) Topological Vector Spaces, Second Edition (Chapman & Hall/CRC Pure and Applied Mathematics) Environmental and Ecological Statistics with R, Second Edition (Chapman & Hall/CRC Applied Environmental Statistics) Introduction to Stochastic Processes (Chapman & Hall/CRC Probability Series) Linear Models with R, Second Edition (Chapman & Hall/CRC Texts in Statistical Science) Generalized Linear Models, Second Edition (Chapman & Hall/CRC Monographs on Statistics & Applied Probability) Machine Learning: An Algorithmic Perspective, Second Edition (Chapman & Hall/Crc Machine Learning & Pattern Recognition) Introduction to Set Theory, Third Edition, Revised and Expanded (Chapman & Hall/CRC Pure and Applied Mathematics) Modern Data Science with R (Chapman & Hall/CRC Texts in Statistical Science) Introduction to Proteins: Structure, Function, and Motion (Chapman & Hall/CRC Mathematical and Computational Biology) An Introduction to Systems Biology: Design Principles of Biological Circuits (Chapman & Hall/CRC Mathematical and Computational Biology)