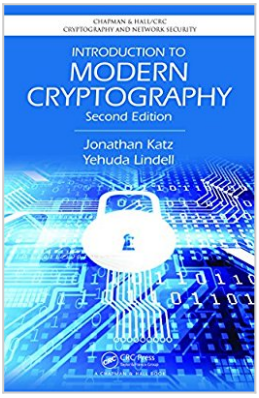

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series)

By Jonathan Katz, Yehuda Lindell

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell

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.

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

By Jonathan Katz, Yehuda Lindell

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell

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.

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell Bibliography

- Sales Rank: #597018 in eBooks
- Published on: 2014-11-06
- Released on: 2014-11-06
- Format: Kindle eBook

Editorial Review

Review

"The work is comprehensive, rigorous, and yet accessible for dedicated students."
?*Computing Reviews*, October 2015

"… 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. … 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. … This textbook is appropriate for use in teaching at either an advanced undergraduate or graduate level … 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 accessible?**Introduction to Modern Cryptography** achieves this admirably."
?*Mathematical Reviews*, August 2015

Praise for the First Edition:
"This book is a comprehensive, rigorous introduction to what the authors name ‘modern’ cryptography. … a novel approach to how cryptography is taught, replacing the older, construction-based approach. … The concepts are clearly stated, both in an intuitive fashion and formally. … I would heartily recommend this book to anyone who is interested in cryptography. … The exercises are challenging and interesting, and can benefit readers of all academic levels."
?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."
?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."
?Donald L. Vestal, South Dakota State University, Brookings, USA, *MAA Online*, July 2008

"… 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."

?Steven D. Galbraith, *Mathematical Reviews*, 2009

"The book is highly recommended as a textbook in cryptography courses at graduate or advanced undergraduate levels. … 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." ?Guillermo Morales-Luna, *Zentralblatt MATH*, Vol. 1143

About the Author

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.

Users Review

From reader reviews:

Larry Murray:

Typically the book Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) will bring one to the new experience of reading the book. The author style to spell out the idea is very unique. When you try to find new book to read, this book very suitable to you. The book Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) is much recommended to you to study. You can also get the e-book through the official web site, so you can quickly to read the book.

Jamie Treat:

The guide untitled Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) is the publication that recommended to you to learn. You can see the quality of the guide content that will be shown to you. The language that author use to explained their ideas are easily to understand. The writer was did a lot of investigation when write the book, so the information that they share to your account is absolutely accurate. You also can get the e-book of Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) from the publisher to make you considerably more enjoy free time.

Joe Dix:

The reason why? Because this Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) is an unordinary book that the inside of the e-book waiting for you to snap the item but latter it will distress you with the secret it inside. Reading this book beside it was fantastic author who all write the book in such remarkable way makes the content interior easier to understand, entertaining approach but still convey the meaning fully. So , it is good for you for not hesitating having this nowadays or you going to regret it. This book will give you a lot of benefits than the other book possess such as help improving your proficiency and your critical thinking technique. So , still want to delay having that book? If I have been you I will go to the reserve store hurriedly.

Eddie McCoy:

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) can be one of your basic books that are good idea. Many of us recommend that straight away because this guide has good vocabulary that can increase your knowledge in vocab, easy to understand, bit entertaining but still delivering the information. The article author giving his/her effort to set every word into delight arrangement in writing Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) but doesn't forget the main position, giving the reader the hottest in addition to based confirm resource data that maybe you can be considered one of it. This great information may drawn you into brand-new stage of crucial contemplating.

Read Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell for online ebook

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell books to read online.

Online Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell ebook PDF download

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell Doc

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell Mobipocket

Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) By Jonathan Katz, Yehuda Lindell EPub