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

Jonathan Katz, Yehuda Lindell

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

Jonathan Katz, Yehuda Lindell

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

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

---

From reader reviews:

Ann Bland:

Do you one among people who can't read pleasant if the sentence chained within the straightway, hold on guys that aren't like that. This Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) book is readable by simply you who hate those straight word style. You will find the facts here are arrange for enjoyable reading through experience without leaving perhaps decrease the knowledge that want to provide to you. The writer of Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) content conveys objective easily to understand by many individuals. The printed and e-book are not different in the content but it just different such as it. So , do you nevertheless thinking Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) is not loveable to be your top list reading book?

Breanne Gardner:

Typically the book Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) will bring you to definitely the new experience of reading some sort of book. The author style to describe the idea is very unique. If you try to find new book to see, this book very appropriate to you. The book Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) is much recommended to you to learn. You can also get the e-book from the official web site, so you can easier to read the book.

Clyde Connell:

In this time globalization it is important to someone to get information. The information will make someone to understand the condition of the world. The condition of the world makes the information simpler to share. You can find a lot of referrals to get information example: internet, newspaper, book, and soon. You will observe that now, a lot of publisher this print many kinds of book. The actual book that recommended to you personally is Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series) this guide consist a lot of the information of the condition of this world now. This particular book was represented how can the world has grown up. The words styles that writer make usage of to explain it is easy to understand. The particular writer made some research when he makes this book. That is why this book suitable all of you.

Charlie Attwood:

What is your hobby? Have you heard which question when you got learners? We believe that that concern was given by teacher to their students. Many kinds of hobby, Everyone has different hobby. Therefore you know that little person like reading or as reading become their hobby. You need to understand that reading is very important in addition to book as to be the point. Book is important thing to provide you knowledge,

except your personal teacher or lecturer. You will find good news or update regarding something by book. Different categories of books that can you go onto be your object. One of them are these claims Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series).

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