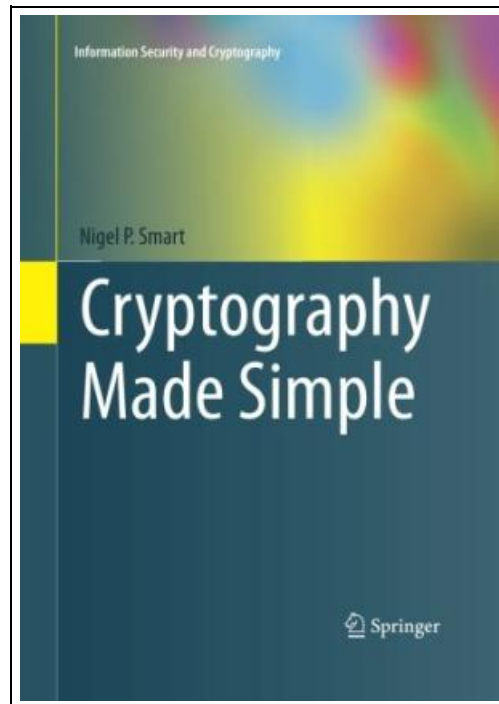


Cryptography Made Simple



Filesize: 3.61 MB

Reviews




The ideal publication i possibly go through. I was able to comprehended every thing out of this published e publication. I am delighted to explain how this is actually the finest pdf i have got read inside my personal existence and could be he very best ebook for possibly.
(Roberto Friesen)

CRYPTOGRAPHY MADE SIMPLE



To download **Cryptography Made Simple** eBook, make sure you follow the button under and download the document or have access to additional information that are highly relevant to CRYPTOGRAPHY MADE SIMPLE ebook.

Condition: New. Publisher/Verlag: Springer, Berlin | In this introductory textbook the author explains the key topics in cryptography. He takes a modern approach, where defining what is meant by "secure" is as important as creating something that achieves that goal, and security definitions are central to the discussion throughout. The author balances a largely non-rigorous style - many proofs are sketched only - with appropriate formality and depth. For example, he uses the terminology of groups and finite fields so that the reader can understand both the latest academic research and "real-world" documents such as application programming interface descriptions and cryptographic standards. The text employs colour to distinguish between public and private information, and all chapters include summaries and suggestions for further reading. This is a suitable textbook for advanced undergraduate and graduate students in computer science, mathematics and engineering, and for self-study by professionals in information security. While the appendix summarizes most of the basic algebra and notation required, it is assumed that the reader has a basic knowledge of discrete mathematics, probability, and elementary calculus. | Modular Arithmetic, Groups, Finite Fields and Probability.- Elliptic Curves.- Historical Ciphers.- The Enigma Machine.- Information Theoretic Security.- Historical Stream Ciphers.- Modern Stream Ciphers.- Block Ciphers.- Symmetric Key Distribution.- Hash Functions and Message Authentication Codes.- Basic Public Key Encryption Algorithms.- Primality Testing and Factoring.- Discrete Logarithms.- Key Exchange and Signature Schemes.- Implementation Issues.- Obtaining Authentic Public Keys.- Attacks on Public Key Schemes.- Definitions of Security.- Complexity Theoretic Approaches.- Provable Security: With Random Oracles.- Hybrid Encryption.- Provable Security: Without Random Oracles.- Secret Sharing Schemes.- Commitments and Oblivious Transfer.- Zero-Knowledge Proofs.- Secure Multiparty Computation. | Format: Paperback | Language/Sprache: english | 935 gr | 257x180x30 mm | 481 pp.

-  [Read Cryptography Made Simple Online](#)
-  [Download PDF Cryptography Made Simple](#)
-  [Download ePub Cryptography Made Simple](#)

See Also

**[PDF] Would It Kill You to Stop Doing That?**

Click the web link listed below to download and read "Would It Kill You to Stop Doing That?" PDF file.

[Download eBook](#)

»

**[PDF] Violet Rose and the Surprise Party**

Click the web link listed below to download and read "Violet Rose and the Surprise Party" PDF file.

[Download eBook](#)

»

**[PDF] What is in My Net? (Pink B) NF**

Click the web link listed below to download and read "What is in My Net? (Pink B) NF" PDF file.

[Download eBook](#)

»

**[PDF] Read Write Inc. Phonics: Purple Set 2 Non-Fiction 4 What is it?**

Click the web link listed below to download and read "Read Write Inc. Phonics: Purple Set 2 Non-Fiction 4 What is it?" PDF file.

[Download eBook](#)

»

**[PDF] Public Opinion + Conducting Empirical Analysis**

Click the web link listed below to download and read "Public Opinion + Conducting Empirical Analysis" PDF file.

[Download eBook](#)

»

**[PDF] Two Treatises: The Pearle of the Gospell, and the Pilgrims Profession to Which Is Added a Glasse for Gentlewomen to Dresse Themselves By. by Thomas Taylor Preacher of Gods Word to the Towne of Reding. (1624-1625)**

Click the web link listed below to download and read "Two Treatises: The Pearle of the Gospell, and the Pilgrims Profession to Which Is Added a Glasse for Gentlewomen to Dresse Themselves By. by Thomas Taylor Preacher of Gods Word to the Towne of Reding. (1624-1625)" PDF file.

[Download eBook](#)

»

**[PDF] Star Flights Bedtime Spaceship: Journey Through Space While Drifting Off to Sleep**

Access the hyperlink beneath to get "Star Flights Bedtime Spaceship: Journey Through Space While Drifting Off to Sleep" PDF document.

[Save PDF](#)

»

**[PDF] YJ] New primary school language learning counseling language book of knowledge [Genuine Specials(Chinese Edition)**

Access the hyperlink beneath to get "YJ] New primary school language learning counseling language book of knowledge [Genuine Specials(Chinese Edition)" PDF document.

[Save PDF](#)

»

**[PDF] Iceland**

Access the hyperlink beneath to get "Iceland" PDF document.

[Save PDF](#)

»

**[PDF] Chaucer's Canterbury Tales**

Access the hyperlink beneath to get "Chaucer's Canterbury Tales" PDF document.

[Save PDF](#)

»

**[PDF] I Learn, I Speak: Basic Skills for Preschool Learners of English and Chinese**

Access the hyperlink beneath to get "I Learn, I Speak: Basic Skills for Preschool Learners of English and Chinese" PDF document.

[Save PDF](#)

»

**[PDF] Medical information retrieval (21 universities and colleges teaching information literacy education family planning)**

Access the hyperlink beneath to get "Medical information retrieval (21 universities and colleges teaching information literacy education family planning)" PDF document.

[Save PDF](#)

»