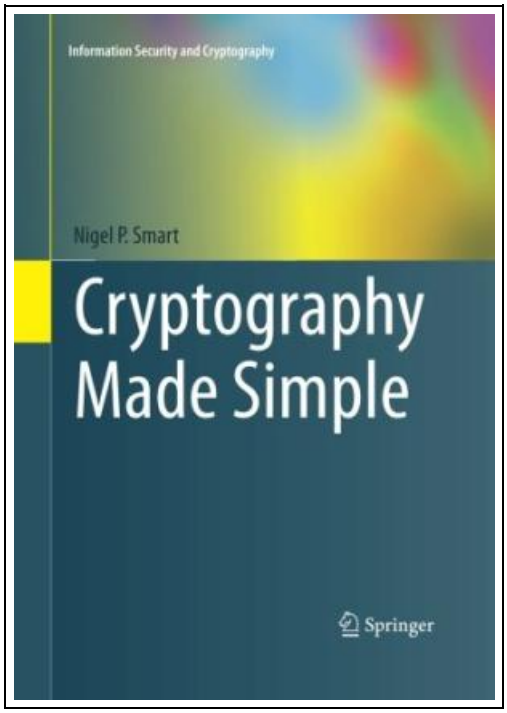
# Cryptography Made Simple




Filesize: 6.07 MB

### *Reviews*

*The very best ebook i ever study. It really is rally fascinating throgh reading through period of time. It is extremely difficult to leave it before concluding, once you begin to read the book.*
***(Coleman Kreiger)***

# CRYPTOGRAPHY MADE SIMPLE

DOWNLOAD PDF

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

## You May Also Like

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

Pearson Education Limited. Book Condition: New. This title is part of Pearson's Bug Club - the first whole-school reading programme that joins books and an online reading world to teach today's children to read. In...

Read Document »

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

Oxford University Press, United Kingdom, 2016. Paperback. Book Condition: New. 215 x 108 mm. Language: N/A. Brand New Book. These decodable non-fiction books provide structured practice for children learning to read. Each set of books...

Read Document »

**What is Love A Kid Friendly Interpretation of 1 John 311, 16-18 1 Corinthians 131-8 13**

Teaching Christ's Children Publishing. Paperback. Book Condition: New. Daan Yahya (illustrator). Paperback. 26 pages. Dimensions: 10.0in. x 8.0in. x 0.1in.What is Love is a Bible based picture book that is designed to help children understand...

Read Document »

**Not for Spies] - What Is a Human Being Part2: Continued**

Createspace Independent Publishing Platform, United States, 2015. Paperback. Book Condition: New. Expanded. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.PART2 of [NOT FOR SPIES] WHAT IS A HUMAN...

Read Document »

**Not for Spies] - What Is a Human Being?**

Createspace, United States, 2013. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.5th EXTENDED EDITION ---------- DO.YOU.HAVE. THE SLIGHTEST IDEA WHAT I JUST GAVE YOU?...

Read Document »

**Broken: I Was Just Five Years Old When My Father Abused Me and Robbed Me of My Childhood. This is My True Story of How I Never Gave Up on Hope and Happiness.**

John Blake Publishing Ltd, 2013. Paperback. Book Condition: New. Brand new book. DAILY dispatch from our warehouse in Sussex, all international orders sent Airmail. We're happy to offer significant POSTAGE DISCOUNTS for MULTIPLE ITEM orders.

Save PDF »

**Heaven is for Real for Little Ones**

Thomas Nelson. Hardcover. Book Condition: New. Board book. 26 pages. Dimensions: 7.1in. x 5.3in. x 0.7in.Heaven is for real, and you are going to like it! Colton Burpo came back from his trip to heaven

Save PDF »

**Books are well written, or badly written. That is all.**

GRIN Verlag Okt 2013, 2013. Taschenbuch. Book Condition: Neu. 210x148x1 mm. This item is printed on demand - Print on Demand Neuware - Essay from the year 2007 in the subject English - Literature, Works,

Save PDF »

**Because It Is Bitter, and Because It Is My Heart (Plume)**

Plume. PAPERBACK. Book Condition: New. 0452265819 12+ Year Old paperback book-Never Read-may have light shelf or handling wear-has a price sticker or price written inside front or back cover-publishers mark-Good Copy- I ship FAST with

Save PDF »

**Cheesie Mack Is Running Like Crazy!**

Random House USA Inc, United States, 2014. Paperback. Book Condition: New. Douglas Holgate (illustrator). Reprint. 190 x 135 mm. Language: English . Brand New Book. Readers of Diary of a Wimpy Kid will love Cheesie

Save PDF »