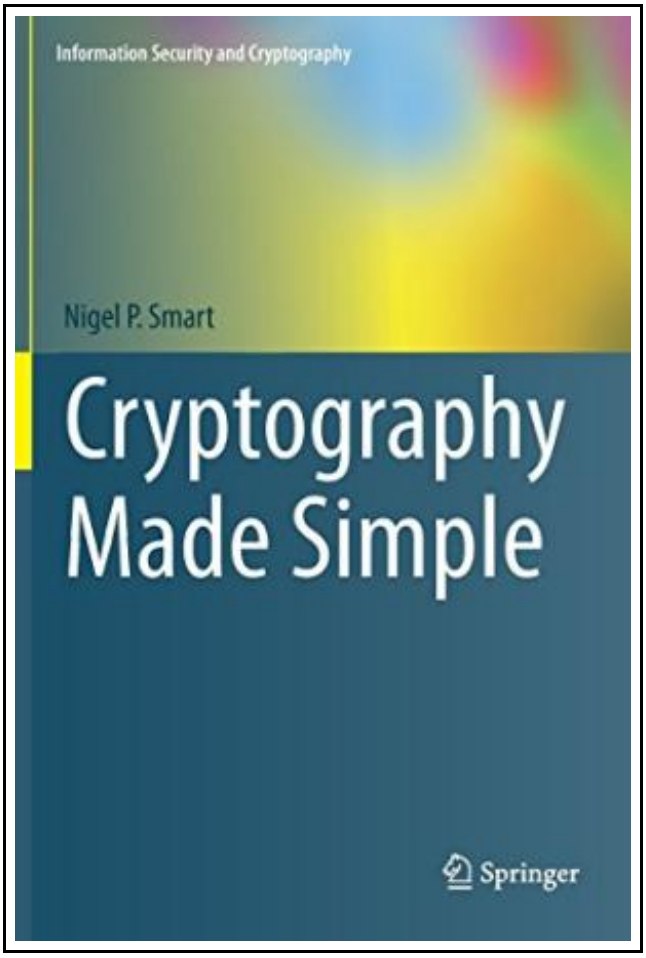
Cryptography Made Simple: 2016



Filesize: 6.79 MB

Reviews

Certainly, this is the finest job by any publisher. I was able to comprehended almost everything out of this published e ebook. You wont truly feel monotony at at any moment of the time (that's what catalogues are for concerning should you question me).

(Graciela Emard)

CRYPTOGRAPHY MADE SIMPLE: 2016

Springer International Publishing AG. Hardback. Book Condition: new. BRAND NEW, Cryptography Made Simple: 2016, Nigel P. Smart, 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 chapters in Part 1 offer a brief introduction to the mathematical foundations: modular arithmetic, groups, finite fields, and probability; primality testing and factoring; discrete logarithms; elliptic curves; and lattices. Part 2 of the book shows how historical ciphers were broken, thus motivating the design of modern cryptosystems since the 1960s; this part also includes a chapter on information-theoretic security. Part 3 covers the core aspects of modern cryptography: the definition of security; modern stream ciphers; block ciphers and modes of operation; hash functions, message authentication codes, and key derivation functions; the "naive" RSA algorithm; public key encryption and signature algorithms; cryptography based on computational complexity; and certificates, key transport and key agreement. Finally, Part 4 addresses advanced prot ocols, where the parties may have different or even conflicting security goals: secret sharing schemes; commitments and oblivious transfer; zero-knowledge proofs; and secure multi-party computation. 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...

Other Kindle Books

Book Finds: How to Find, Buy, and Sell Used and Rare Books (Revised)

Perigee. PAPERBACK. Book Condition: New. 0399526544 Never Read-12+ year old Paperback book with dust jacket-may have light shelf or handling wear-has a price sticker or price written inside front or back cover-publishers mark-Good Copy- I...

Read ePub »

Edible Bible Crafts: 64 Delicious Story-Based Craft Ideas for Children

BRF (The Bible Reading Fellowship). Paperback. Book Condition: new. BRAND NEW, Edible Bible Crafts: 64 Delicious Story-Based Craft Ideas for Children, Sally Welch, If you're looking for child-friendly Bible-themed cooking activities, this is the book...

Read ePub »

Bully, the Bullied, and the Not-So Innocent Bystander: From Preschool to High School and Beyond: Breaking the Cycle of Violence and Creating More Deeply Caring Communities (Paperback)

HarperCollins Publishers Inc, United States, 2016. Paperback. Book Condition: New. Reprint. 203 x 135 mm. Language: English . Brand New Book. An international bestseller, Barbara Coloroso s groundbreaking and trusted guide on bullying-including cyberbullying-arms parents...

Read ePub »

THE Key to My Children Series: Evan s Eyebrows Say Yes (Paperback)

AUTHORHOUSE, United States, 2006. Paperback. Book Condition: New. 274 x 216 mm. Language: English . Brand New Book ***** Print on Demand *****.THE KEY TO MY CHILDREN SERIES: EVAN S EYEBROWS SAY YES is about...

Read ePub »

Six Steps to Inclusive Preschool Curriculum: A UDL-Based Framework for Children's School Success

Brookes Publishing Co. Paperback. Book Condition: new. BRAND NEW, Six Steps to Inclusive Preschool Curriculum: A UDL-Based Framework for Children's School Success, Eva M. Horn, Susan B. Palmer, Gretchen D. Butera, Joan A. Lieber, How...

Read ePub »

JA] early childhood parenting :1-4 Genuine Special(Chinese Edition)

paperback. Book Condition: New. Ship out in 2 business day, And Fast shipping, Free Tracking number will be provided after the shipment.Paperback. Pub Date :2006-01-01 Pages: 179 Publisher: the China Pictorial Our book is all

Save Document »

The 32 Stops: The Central Line

Penguin Books Ltd. Paperback. Book Condition: new. BRAND NEW, The 32 Stops: The Central Line, Danny Dorling, Geographer Danny Dorling tells the stories of the people who live along The 32 Stops of the Central

Save Document »

Read Write Inc. Phonics: Green Set 1 Non-Fiction 5 Camping (Paperback)

Oxford University Press, United Kingdom, 2016. Paperback. Book Condition: New. 210 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

Save Document »

A Parent s Guide to STEM (Paperback)

U.S. News World Report, United States, 2015. Paperback. Book Condition: New. 214 x 149 mm. Language: English . Brand New Book ***** Print on Demand *****.This lively, colorful guidebook provides everything you need to know

Save Document »

Good Tempered Food: Recipes to love, leave and linger over

Clearview. Paperback. Book Condition: new. BRAND NEW, Good Tempered Food: Recipes to love, leave and linger over, Tamasin Day-Lewis, Slow-cooked food and what the author likes to call 'good tempered food', is what proper cooking

Save Document »