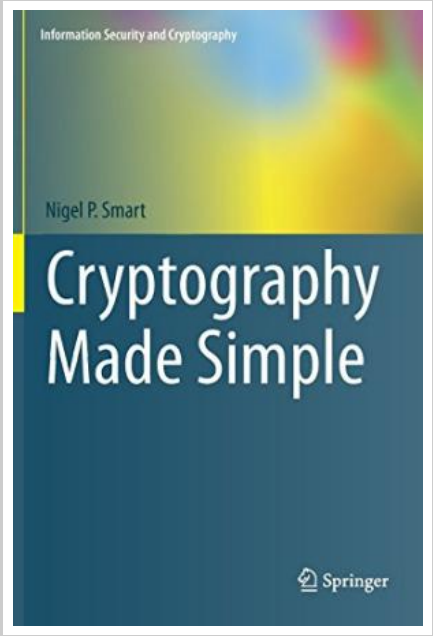

Cryptography Made Simple: 2016

By Nigel P. Smart

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;...

Reviews

The book is easy in study easier to comprehend. I have study and that i am certain that i will gonna read once again once again in the foreseeable future. Your lifestyle span will likely be transform the instant you comprehensive reading this pdf.

-- ***Dr. Jaydon Mosciski***

This publication may be worthy of a read through, and a lot better than other. It is among the most incredible book we have read through. Your daily life period will be change when you total reading this article publication.

-- ***Garett Baumbach***

Related eBooks

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 ship FAST with FREE tracking!! * I...

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 for you! Sally Welch brings the Bible...

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

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 and teachers with real solutions for a...

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

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 a three year old little boy who...

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 can inclusive early educators plan and deliver...

A Smarter Way to Learn JavaScript: The New Approach That Uses Technology to Cut Your Effort in Half

Createspace, United States, 2014. Paperback. Book Condition: New. 251 x 178 mm. Language: English . Brand New Book ***** Print on Demand *****.The ultimate learn-by-doing approachWritten for beginners, useful for experienced developers who want to sharpen their skills and don t mind...