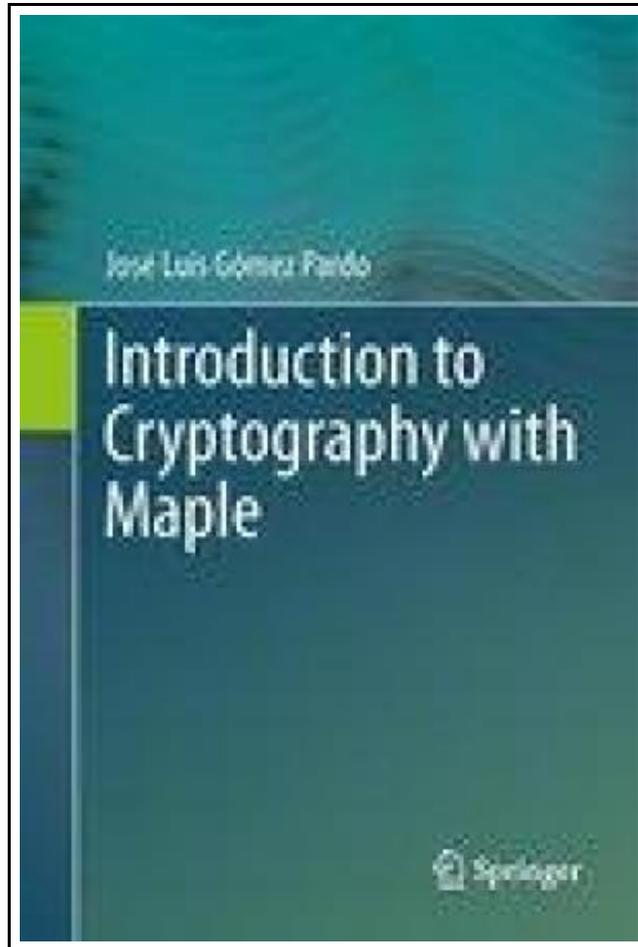


Introduction to Cryptography with Maple



Filesize: 3.71 MB

Reviews

Completely essential read through ebook. This can be for all who statte there was not a well worth reading. You wont really feel monotony at at any time of your own time (that's what catalogs are for relating to if you request me).

(Maud Mitchell)

INTRODUCTION TO CRYPTOGRAPHY WITH MAPLE



Springer Dez 2012, 2012. Buch. Book Condition: Neu. 23.5x15.5x cm. This item is printed on demand - Print on Demand Neuware - This introduction to cryptography employs a programming-oriented approach to study the most important cryptographic schemes in current use and the main cryptanalytic attacks against them. Discussion of the theoretical aspects, emphasizing precise security definitions based on methodological tools such as complexity and randomness, and of the mathematical aspects, with emphasis on number-theoretic algorithms and their applications to cryptography and cryptanalysis, is integrated with the programming approach, thus providing implementations of the algorithms and schemes as well as examples of realistic size. A distinctive feature of the author's approach is the use of Maple as a programming environment in which not just the cryptographic primitives but also the most important cryptographic schemes are implemented following the recommendations of standards bodies such as NIST, with many of the known cryptanalytic attacks implemented as well. The purpose of the Maple implementations is to let the reader experiment and learn, and for this reason the author includes numerous examples. The book discusses important recent subjects such as homomorphic encryption, identity-based cryptography and elliptic curve cryptography. The algorithms and schemes which are treated in detail and implemented in Maple include AES and modes of operation, CMAC, GCM/GMAC, SHA-256, HMAC, RSA, Rabin, Elgamal, Paillier, Cocks IBE, DSA and ECDSA. In addition, some recently introduced schemes enjoying strong security properties, such as RSA-OAEP, Rabin-SAEP, Cramer--Shoup, and PSS, are also discussed and implemented. On the cryptanalysis side, Maple implementations and examples are used to discuss many important algorithms, including birthday and man-in-the-middle attacks, integer factorization algorithms such as Pollard's rho and the quadratic sieve, and discrete log algorithms such as baby-step giant-step, Pollard's rho, Pohlig--Hellman and the index calculus method. This textbook is suitable for advanced...



[Read Introduction to Cryptography with Maple Online](#)



[Download PDF Introduction to Cryptography with Maple](#)

Relevant Books



Unplug Your Kids: A Parent's Guide to Raising Happy, Active and Well-Adjusted Children in the Digital Age

Adams Media Corporation. Paperback. Book Condition: new. BRAND NEW, Unplug Your Kids: A Parent's Guide to Raising Happy, Active and Well-Adjusted Children in the Digital Age, David Dutwin, TV. Web Surfing. IMing. Text Messaging. Video...

[Read PDF »](#)



Kindergarten Culture in the Family and Kindergarten; A Complete Sketch of Froebel s System of Early Education, Adapted to American Institutions. for the Use of Mothers and Teachers (Paperback)

Rarebooksclub.com, United States, 2012. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book ***** Print on Demand *****.This historic book may have numerous typos and missing text. Purchasers can download...

[Read PDF »](#)



The Sunday Kindergarten Game Gift and Story: A Manual for Use in the Sunday, Schools and in the Home (Classic Reprint) (Paperback)

Forgotten Books, United States, 2015. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****.Excerpt from The Sunday Kindergarten Game Gift and Story: A Manual for...

[Read PDF »](#)



California Version of Who Am I in the Lives of Children? an Introduction to Early Childhood Education, Enhanced Pearson Etext with Loose-Leaf Version -- Access Card Package

Pearson, United States, 2015. Loose-leaf. Book Condition: New. 10th. 249 x 201 mm. Language: English . Brand New Book. NOTE: Used books, rentals, and purchases made outside of Pearson If purchasing or renting from companies...

[Read PDF »](#)



Who Am I in the Lives of Children? an Introduction to Early Childhood Education, Enhanced Pearson Etext with Loose-Leaf Version -- Access Card Package

Pearson, United States, 2015. Book. Book Condition: New. 10th. 250 x 189 mm. Language: English . Brand New Book. NOTE: Used books, rentals, and purchases made outside of Pearson If purchasing or renting from companies...

[Read PDF »](#)

**My Friend Has Down's Syndrome**

Barron's Educational Series Inc., U.S. Paperback. Book Condition: new. BRAND NEW, My Friend Has Down's Syndrome, Jennifer Moore-Mallinos, Younger children are normally puzzled when they encounter other kids who suffer from Down's Syndrome. Here is a

[Download Document »](#)

**The Monster Next Door - Read it Yourself with Ladybird: Level 2**

Penguin Books Ltd. Paperback. Book Condition: new. BRAND NEW, The Monster Next Door - Read it Yourself with Ladybird: Level 2, The Monster Next Door, George wants to be a monster, just like his neighbour

[Download Document »](#)

**The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds**

Anness Publishing. Paperback. Book Condition: new. BRAND NEW, The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds, Nicola Baxter, Geoff Ball, This is a super-size first reading book for 3-5 year

[Download Document »](#)

**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) (Paperback)**

Proquest, Eebo Editions, United States, 2010. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book ***** Print on Demand *****.EARLY HISTORY OF RELIGION. Imagine holding history in your hands. Now

[Download Document »](#)

**Read Write Inc. Phonics: Yellow Set 5 Storybook 7 Do We Have to Keep it? (Paperback)**

Oxford University Press, United Kingdom, 2016. Paperback. Book Condition: New. Tim Archbold (illustrator). 211 x 101 mm. Language: N/A. Brand New Book. These engaging Storybooks provide structured practice for children learning to read the Read

[Download Document »](#)