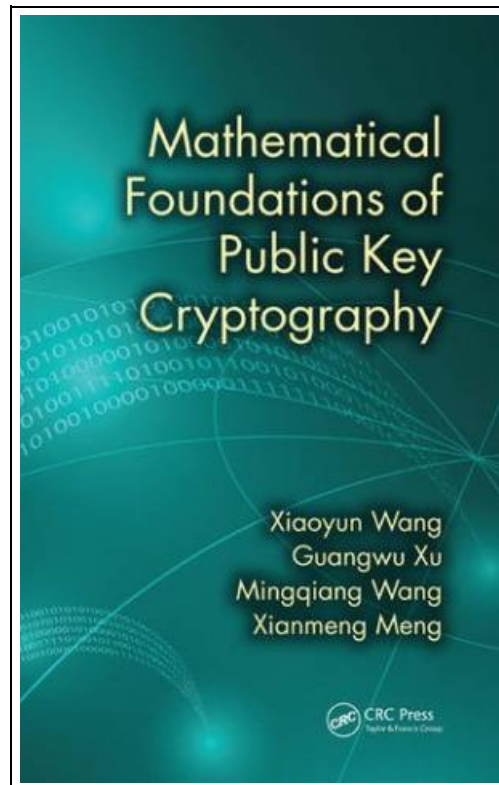


Mathematical Foundations of Public Key Cryptography (Hardback)



Filesize: 6.94 MB

Reviews

A whole new e book with a brand new point of view. I could possibly comprehend every thing using this written e book. Its been written in an extremely simple way which is only soon after i finished reading through this ebook by which actually modified me, change the way in my opinion.

(Marcia McDermott)

MATHEMATICAL FOUNDATIONS OF PUBLIC KEY CRYPTOGRAPHY (HARDBACK)



Taylor Francis Inc, United States, 2015. Hardback. Condition: New. Language: English . Brand New Book. In Mathematical Foundations of Public Key Cryptography, the authors integrate the results of more than 20 years of research and teaching experience to help students bridge the gap between math theory and crypto practice. The book provides a theoretical structure of fundamental number theory and algebra knowledge supporting public-key cryptography. Rather than simply combining number theory and modern algebra, this textbook features the interdisciplinary characteristics of cryptography-revealing the integrations of mathematical theories and public-key cryptographic applications. Incorporating the complexity theory of algorithms throughout, it introduces the basic number theoretic and algebraic algorithms and their complexities to provide a preliminary understanding of the applications of mathematical theories in cryptographic algorithms. Supplying a seamless integration of cryptography and mathematics, the book includes coverage of elementary number theory; algebraic structure and attributes of group, ring, and field; cryptography-related computing complexity and basic algorithms, as well as lattice and fundamental methods of lattice cryptanalysis. The text consists of 11 chapters. Basic theory and tools of elementary number theory, such as congruences, primitive roots, residue classes, and continued fractions, are covered in Chapters 1-6. The basic concepts of abstract algebra are introduced in Chapters 7-9, where three basic algebraic structures of groups, rings, and fields and their properties are explained. Chapter 10 is about computational complexities of several related mathematical algorithms, and hard problems such as integer factorization and discrete logarithm. Chapter 11 presents the basics of lattice theory and the lattice basis reduction algorithm-the LLL algorithm and its application in the cryptanalysis of the RSA algorithm. Containing a number of exercises on key algorithms, the book is suitable for use as a textbook for undergraduate students and first-year graduate students in information security programs. It is also an ideal...



[Read Mathematical Foundations of Public Key Cryptography \(Hardback\) Online](#)
[Download PDF Mathematical Foundations of Public Key Cryptography \(Hardback\)](#)

See Also



Everything Ser The Everything Green Baby Book From Pregnancy to Babys First Year An Easy and Affordable Guide to Help Moms Care for Their Baby And for the Earth by Jenn Savedge 2009 Paperback

Book Condition: Brand New. Book Condition: Brand New.

[Save PDF »](#)



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 SEYEBROWS SAY YES is about...

[Save PDF »](#)



Basic Concepts, Grade Preschool

Book Condition: Brand New. Book Condition: Brand New.

[Save PDF »](#)



I Learn, I Speak: Basic Skills for Preschool Learners of English and Chinese

Paraxus International, Inc., United States, 2012. Paperback. Book Condition: New. 279 x 216 mm. Language: English . Brand New Book ***** Print on Demand *****.Please go to // and shapes for some high resolution sample...

[Save PDF »](#)



Access2003 Chinese version of the basic tutorial (secondary vocational schools teaching computer series)

paperback. Book Condition: New. Ship out in 2 business day, And Fast shipping, Free Tracking number will be provided after the shipment. Pages Number: 192 Publisher: People's Post Pub. Date :2011-10-01 version 1. Access 2003 Tutorial...

[Save PDF »](#)