



Mathematical Foundations of Public Key Cryptography

Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng

Download now

[Click here](#) if your download doesn't start automatically

Mathematical Foundations of Public Key Cryptography

Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng

Mathematical Foundations of Public Key Cryptography Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng

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 reference book for cryptography professionals looking to master public-key cryptography.

 [Download Mathematical Foundations of Public Key Cryptograph ...pdf](#)

 [Read Online Mathematical Foundations of Public Key Cryptogra ...pdf](#)

Download and Read Free Online Mathematical Foundations of Public Key Cryptography Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng

From reader reviews:

Frances Norman:

Do you considered one of people who can't read satisfying if the sentence chained from the straightway, hold on guys this specific aren't like that. This Mathematical Foundations of Public Key Cryptography book is readable by simply you who hate the perfect word style. You will find the data here are arrange for enjoyable studying experience without leaving also decrease the knowledge that want to give to you. The writer involving Mathematical Foundations of Public Key Cryptography content conveys objective easily to understand by many individuals. The printed and e-book are not different in the information but it just different in the form of it. So , do you nonetheless thinking Mathematical Foundations of Public Key Cryptography is not loveable to be your top checklist reading book?

Marlene Turner:

The actual book Mathematical Foundations of Public Key Cryptography has a lot details on it. So when you check out this book you can get a lot of gain. The book was compiled by the very famous author. Mcdougal makes some research ahead of write this book. This book very easy to read you can obtain the point easily after scanning this book.

Anita Rhodes:

Playing with family in the park, coming to see the marine world or hanging out with friends is thing that usually you could have done when you have spare time, in that case why you don't try factor that really opposite from that. One activity that make you not experiencing tired but still relaxing, trilling like on roller coaster you have been ride on and with addition details. Even you love Mathematical Foundations of Public Key Cryptography, it is possible to enjoy both. It is very good combination right, you still want to miss it? What kind of hangout type is it? Oh can occur its mind hangout guys. What? Still don't have it, oh come on its named reading friends.

Joseph Russell:

The book untitled Mathematical Foundations of Public Key Cryptography contain a lot of information on the idea. The writer explains your ex idea with easy technique. The language is very clear to see all the people, so do not necessarily worry, you can easy to read that. The book was published by famous author. The author will take you in the new time of literary works. You can read this book because you can continue reading your smart phone, or gadget, so you can read the book in anywhere and anytime. If you want to buy the e-book, you can available their official web-site along with order it. Have a nice learn.

**Download and Read Online Mathematical Foundations of Public
Key Cryptography Xiaoyun Wang, Guangwu Xu, Mingqiang Wang,
Xianmeng Meng #23DINSEFWJG**

Read Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng for online ebook

Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng Free PDF download, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng books to read online.

Online Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng ebook PDF download

Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng Doc

Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng Mobipocket

Mathematical Foundations of Public Key Cryptography by Xiaoyun Wang, Guangwu Xu, Mingqiang Wang, Xianmeng Meng EPub