Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security)

Song Y. Yan

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security)

Song Y. Yan

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) Song Y. Yan
Primality testing and integer factorization, as identified by Gauss in his "Disquisitiones Arithmeticae", Article 329, in 1801, are the two most fundamental problems (as well as the two most important research fields) in computational number theory. With the advent of modern computers, unexpected applications have also been found in primality testing and integer factorization.
Primality Testing and Integer Factorization in Public-Key Cryptography introduces various algorithms for primality testing and integer factorization, with their applications in public-key cryptography and information security. More specifically, this book explores basic concepts and results in number theory in Chapter 1. Chapter 2 discusses various algorithms for primality testing and prime number generation, with an emphasis on the Miller-Rabin probabilistic test, the Goldwasser-Kilian and Atkin-Morain elliptic curve tests, and the Agrawal-Kayal-Saxena deterministic test for primality. Chapter 3 introduces various algorithms, particularly the Elliptic Curve Method (ECM), the Quadratic Sieve (QS) and the Number Field Sieve (NFS) for integer factorization. This chapter also discusses some other computational problems that are related to factoring, such as the square root problem, the discrete logarithm problem and the quadratic residuosity problem. The final chapter presents the applications of the problems/techniques of primality testing, integer factorization, square roots, discrete logarithms and quadratic residuosity in public-key cryptography.
Primality Testing and Integer Factorization in Public-Key Cryptography is designed for a professional audience composed of researchers and practitioners in industry. This book is also suitable as a secondary text for graduate-level students in computer science, mathematics and engineering.

Download and Read Free Online Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) Song Y. Yan

---

From reader reviews:

Michael Jackson:

Do you have favorite book? If you have, what is your favorite's book? Book is very important thing for us to be aware of everything in the world. Each e-book has different aim or goal; it means that reserve has different type. Some people experience enjoy to spend their a chance to read a book. They are reading whatever they have because their hobby will be reading a book. Think about the person who don't like examining a book? Sometime, particular person feel need book if they found difficult problem or even exercise. Well, probably you will need this Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security).

Lola Hernandez:

The book Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) gives you the sense of being enjoy for your spare time. You may use to make your capable more increase. Book can for being your best friend when you getting pressure or having big problem with the subject. If you can make reading through a book Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) being your habit, you can get considerably more advantages, like add your capable, increase your knowledge about a number of or all subjects. You could know everything if you like available and read a e-book Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security). Kinds of book are several. It means that, science book or encyclopedia or other folks. So , how do you think about this e-book?

David Yoon:

Reading can called head hangout, why? Because if you are reading a book mainly book entitled Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) your head will drift away trough every dimension, wandering in each aspect that maybe mysterious for but surely can become your mind friends. Imaging each word written in a guide then become one application form conclusion and explanation in which maybe you never get prior to. The Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) giving you yet another experience more than blown away your mind but also giving you useful data for your better life on this era. So now let us show you the relaxing pattern the following is your body and mind will probably be pleased when you are finished examining it, like winning a game. Do you want to try this extraordinary spending spare time activity?

William Henderson:

Are you kind of hectic person, only have 10 or even 15 minute in your moment to upgrading your mind talent or thinking skill even analytical thinking? Then you are receiving problem with the book than can satisfy your short period of time to read it because all this time you only find e-book that need more time to

be learn. Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) can be your answer since it can be read by a person who have those short free time problems.

Read Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan for online ebook

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan Free PDF d0wnl0ad, 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 Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan books to read online.

Online Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan ebook PDF download

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan Doc

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan Mobipocket

Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security) by Song Y. Yan EPub