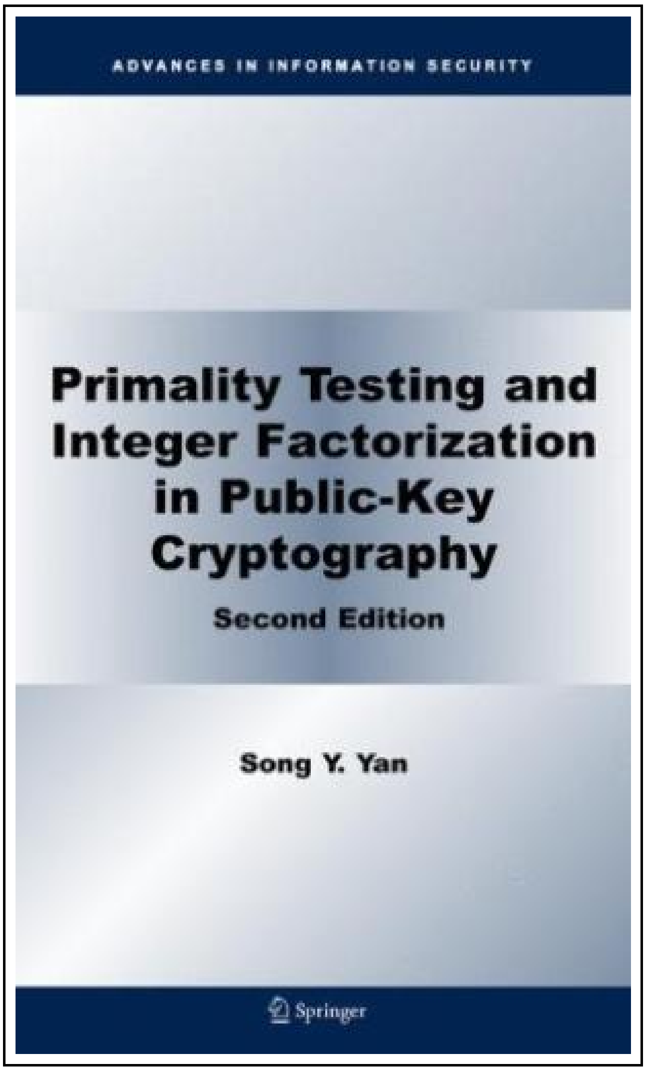
Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security)


ADVANCES IN INFORMATION SECURITY
Primality Testing and Integer Factorization in Public-Key Cryptography
Second Edition
Song Y. Yan
Springer

Filesize: 6.29 MB

Reviews

This kind of publication is every thing and got me to searching in advance and much more. It really is simplistic but surprises within the 50 percent from the ebook. I am easily could get a satisfaction of studying a composed publication.
(Orval Halvorson III)

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY (ADVANCES IN INFORMATION SECURITY)

Springer, 2009. Hardcover. Book Condition: New. Although the Primality Testing Problem (PTP) has been proved to be solvable in deterministic polynomial-time (P) in 2002 by Agrawal, Kayal and Saxena, the Integer Factorization Problem (IFP) still remains unsolvable in P. The security of many practical Public-Key Cryptosystems and Protocols such as RSA (invented by Rivest, Shamir and Adleman) relies on the computational intractability of IFP. This monograph provides a survey of recent progress in Primality Testing and Integer Factorization, with implications to factoring-based Public Key Cryptography. Notable features of this second edition are the several new sections and more than 100 new pages that are added. These include a new section in Chapter 2 on the comparison of Rabin-Miller probabilistic test in RP, Atkin-Morain elliptic curve test in ZPP and AKS deterministic test in P; a new section in Chapter 3 on recent work in quantum factoring; and a new section in Chapter 4 on post-quantum cryptography. To make the book suitable as an advanced undergraduate and/or postgraduate text/reference, about ten problems at various levels of difficulty are added at the end of each section, making about 300 problems in total contained in the book; most of the problems are research-oriented with prizes ordered by individuals or organizations to a total amount over five million US dollars. Primality Testing and Integer Factorization in Public Key Cryptography is designed for practitioners and researchers in industry and graduate-level students in computer science and mathematics.

Relevant Kindle Books

[PDF] Gypsy Breynton

Click the hyperlink under to download "Gypsy Breynton" PDF document.

Save eBook »

[PDF] Memoirs of Robert Cary, Earl of Monmouth

Click the hyperlink under to download "Memoirs of Robert Cary, Earl of Monmouth" PDF document.

Save eBook »

[PDF] Aeschylus

Click the hyperlink under to download "Aeschylus" PDF document.

Save eBook »

[PDF] Index to the Classified Subject Catalogue of the Buffalo Library; The Whole System Being Adopted from the Classification and Subject Index of Mr. Melvil Dewey, with Some Modifications . (Paperback)

Click the hyperlink under to download "Index to the Classified Subject Catalogue of the Buffalo Library; The Whole System Being Adopted from the Classification and Subject Index of Mr. Melvil Dewey, with Some Modifications . (Paperback)" PDF document.

Save eBook »

[PDF] Polly Oliver s Problem: A Story for Girls (Paperback)

Click the hyperlink under to download "Polly Oliver s Problem: A Story for Girls (Paperback)" PDF document.

Save eBook »

[PDF] Public Opinion + Conducting Empirical Analysis

Click the hyperlink under to download "Public Opinion + Conducting Empirical Analysis" PDF document.

Save eBook »