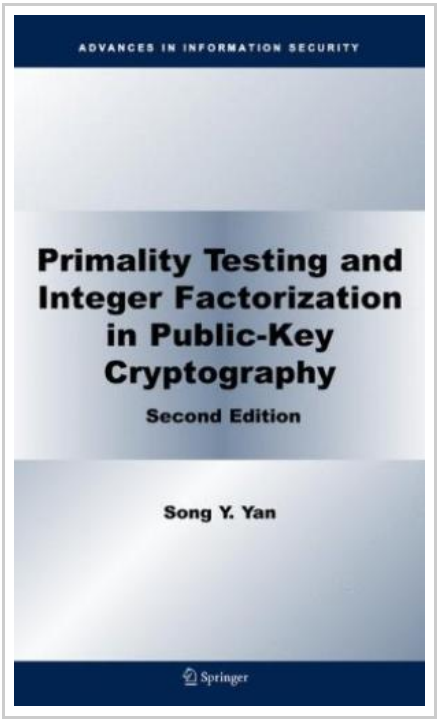

DOWNLOAD

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

By Song Y. Yan

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...

READ ONLINE
[2.06 MB]

Reviews

Comprehensive information! Its this sort of excellent go through. It is packed with knowledge and wisdom You may like just how the author publish this book.

-- ***Mustafa McGlynn***

Complete guideline! Its this kind of great read through. It is probably the most incredible pdf i actually have read through. Its been developed in an extremely straightforward way and it is simply soon after i finished reading this book through which actually modified me, affect the way i really believe.

-- ***Beryl Labadie I***