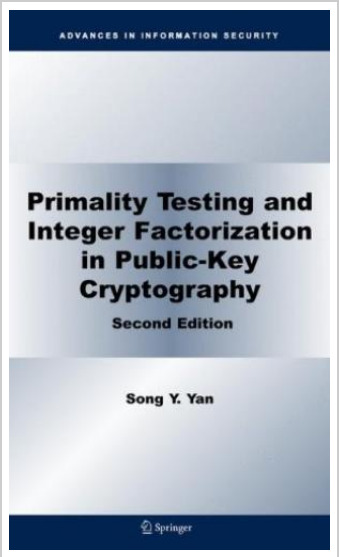




# Primality Testing and Integer Factorization in Public-Key Cryptography (Advances in Information Security)

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...



### Reviews

*Absolutely essential go through pdf. It is writter in simple terms and never difficult to understand. I am just very happy to let you know that this is actually the greatest pdf we have go through in my individual life and might be he greatest pdf for actually.*

-- ***Pete Bosco***

*The best book i at any time read. I am quite late in start reading this one, but better then never. I realized this publication from my dad and i advised this book to understand.*

-- ***Raina Simonis***

## Other PDFs

### 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 .

Rarebooksclub.com, United States, 2013. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book ***** Print on Demand *****.This historic book may have numerous typos and missing text. Purchasers can usually download a free scanned copy of the...

### Dog on It! - Everything You Need to Know about Life Is Right There at Your Feet

14 Hands Press, United States, 2013. Paperback. Book Condition: New. 198 x 132 mm. Language: English . Brand New Book ***** Print on Demand *****.Have you ever told a little white lie? Or maybe a bigger one that wasn t even white?...

### Read Write Inc. Phonics: Orange Set 4 Storybook 2 I Think I Want to be a Bee

Oxford University Press, United Kingdom, 2016. Paperback. Book Condition: New. Tim Archbold (illustrator). 209 x 149 mm. Language: N/A. Brand New Book. These engaging Storybooks provide structured practice for children learning to read the Read Write Inc. Set 1 and 2 sounds....

### Two Treatises: The Pearle of the Gospell, and the Pilgrims Profession to Which Is Added a Glasse for Gentlewomen to Dresse Themselues By. by Thomas Taylor Preacher of Gods Word to the Towne of Reding. (1624-1625)

Proquest, Eebo Editions, United States, 2010. Paperback. Book Condition: New. 246 x 189 mm. Language: English . Brand New Book ***** Print on Demand *****.EARLY HISTORY OF RELIGION. Imagine holding history in your hands. Now you can. Digitally preserved and previously accessible...

### Two Treatises: The Pearle of the Gospell, and the Pilgrims Profession to Which Is Added a Glasse for Gentlewomen to Dresse Themselues By. by Thomas Taylor Preacher of Gods Word to the Towne of Reding. (1625)

Proquest, Eebo Editions, United States, 2010. Paperback. Book Condition: New. 246 x 189 mm. Language: English Brand New Book ***** Print on Demand *****.EARLY HISTORY OF RELIGION. Imagine holding history in your hands. Now you can. Digitally preserved and previously accessible only...

### The About com Guide to Baby Care A Complete Resource for Your Babys Health Development and Happiness by Robin Elise Weiss 2007 Paperback

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