Review of the book

"Primality Testing and Integer Factorization in Public-Key Cryptography"

by Song Y. Yan

Springer 2009 (2^{nd} Edition)

ISBN-13: 978-0-387-77267-7

Dr. Joerg Gerschuetz

2010-01-01

1 What the book is about

This book is a successful compilation of the actual state of research regarding Primality Testing and Integer Factorization, both fundamental problems in number theory having far reaching implications to factoring-based public-key cryptography.

The book itself is divided into four chapters:

① **Number-Theoretic Preliminaries**

This chapter collects the basics of number theory necessary for understanding the following chapters and algorithms. Some of the covered topics are Euclid's algorithm, continued fractions, the Chinese remainder theorem (CRT), quadratic and power residues and some of the essential arithmetic functions. There is also a short introduction into the arithmetic of Elliptic Curves.

② **Primality Testing and Prime Generation**

For a security practitioner this might be the most interesting chapter as it covers the most crucial operations for public-key cryptography. The reader finds a detailed introduction into the most widely used as well as the most recent algorithms for primality testing and reliable prime number generation. One exciting section deals with primality tests for special numbers (Fermat numbers and Mersenne primes).

③ **Integer Factorization and Discrete Logarithms**

Many public-key cryptography schemes rely on the intractability of the integer factorization problem (IFP) or the discrete logarithm problem (DLP). There are still no efficient algorithms for these problems. During the course of the subsections the reader will gain insight into past and recent efforts to solve these, e.g. the Elliptic Curve Method (ECM), the Quadratic Sieve (QS), the Number Field Sieve (NFS), Baby-Step Giant-Step and Index Calculus (just to name the most popular).

④ **Number-Theoretic Cryptography**

The most widely used Cryptographic systems that are based on the number theoretic basics described before are discussed in the final chapter. Among others the reader will find sections on the RSA cryptosystem, its security and cryptanalysis, on Elliptic Curve Cryptography as well as some less known e.g. Rabin or non-factoring based cryptography. There is also a small section dedicated to Zero-Knowledge techniques.

Each chapter is summarized in a closing section which also gives valuable cross references to both standard textbooks and selected essential articles covering the specific topic.

2 What is the book like?

The author knows how to show that "the theory of numbers is one of the most beautiful and pure parts of mathematics" and how to fascinate the reader for this subject. What seems to be a dry and boring mathematical topic at first sight is prepared as an exciting and fascinating story embedded in the world of cryptography known to the security practitioner. This is mainly due to the fact that the text itself is not a stringing together of mathematical formulas and proofs. Instead it is broken up with examples, references to actual work, etc.

Structure and thematic sequence are logical from the first to the last page, new concepts are defined and explained in a coherent manner. The reader neither needs any additional reference to follow the text nor has to be afraid to loose perspective.

It is very pleasant that the bibliography only cites books and articles of essential relevance (about 270 entries - this number has to be compared to several thousand in other textbooks). These are referenced and rated at the end of each chapter, so further reading and involvement is facilitated for the reader not familiar with the matter.

Those readers not so familiar with the subject will find the extensive "List of Notations" at the beginning very valuable.

"One picture is worth ten thousand words", the same holds for a good example! It should be emphasized that throughout the whole book each and every new building block or algorithm is accompanied by at least one elaborated example with detailed solution approach. This makes it an ideal study or reference book for a course dealing with this matter!

3 Would you recommend this book?

The book can be recommended without any restrictions. It is suitable as text book and/or reference book for anybody interested in Primality Testing or Integer Factorization being student, researcher or amateur. As the author prepares the theoretical background in an excellent manner only some familiarity with high-school algebra is needed to follow most parts of the text.

Many examples with detailed calculations help the reader at corners where he might have struggled with the matter. Each section contains a set of problems that encourages the reader to follow up with the topic.

Looking only at the excellent compilation of the number theoretic background and basics in the first chapter the book is worth its price! Other books aim at comparable efforts, but they are either lengthy or incomplete.

From the reviewer's point of view there are only to minor drawbacks:

- Throughout the whole book the same formatting is used for definitions, theorems, proofs, examples, etc., i.e. a bold faced identifier, a text body with identical font size and equal spacing between the items and/or the rest of the text. Each item has its own numbering so that **Definition 1.4.4** might be followed by **Theorem 1.4.7** and **Example 1.4.2**. This makes the text somewhat difficult to read. Using e.g. a smaller font size for the examples, italics, text boxes and comparable format options for the mathematical foundations could result in a more structured and accessible text.
- Solutions for the additional problems in each section are missing. It might be of some help for those who want to dig deeper into some of these problems to have a verified solution available, at least online through a web page.

Nevertheless: This book will definitely not get dusty in the reviewer's book shelf! It will serve as a comprehensive reference of high professional competence. Chapter 1 starts with a citation of Paul Erdös: "*It will be another million years, at least, before we understand the primes.*" - without this book it will be some years more!

The reviewer is a student of Applied IT Security at International School of IT Security, Bochum, Germany.