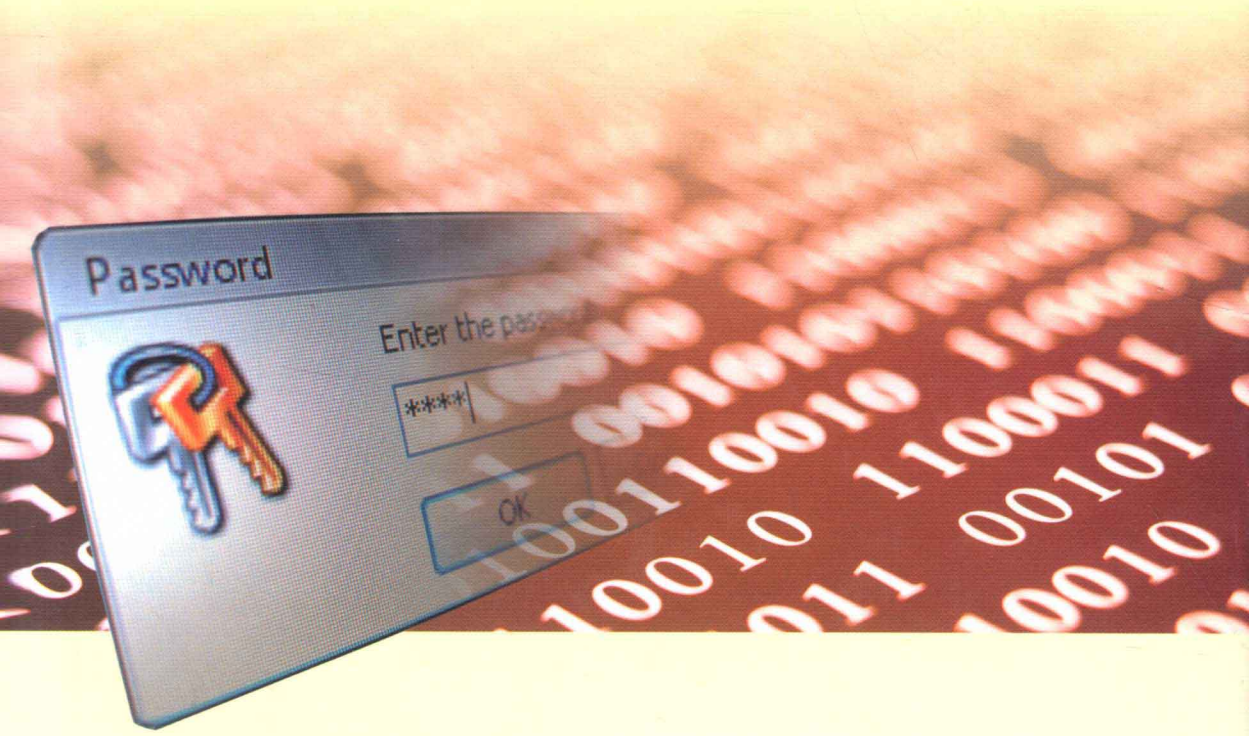
INFORMATION SECURITY SERIES

"十二五"国家重点图书出版规划项目



Song Y. Yan

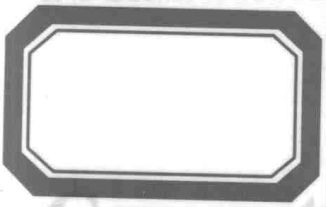
Computational Number Theory and Modern Cryptography

计算数论与现代密码学

高等教育出版社
HIGHER EDUCATION PRESS

“十二五”国家重点图书出版规划项目

INFORMATION SECURITY SERIES



Computational Number Theory and Modern Cryptography

计算数论与现代密码学

JISUAN SHULUN YU XIANDAI MIMAXUE

Song Y. Yan

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

计算数论与现代密码学 = Computational Number Theory and Modern Cryptography : 英文 / 颜松远著
— 北京 : 高等教育出版社, 2013.1
(信息安全系列)
ISBN 978-7-04-034471-4

Ⅰ. ①计… Ⅱ. ①颜… Ⅲ. ①数论-应用-密码算法-研究-英文 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2012)第252943号

策划编辑 陈红英 责任编辑 陈红英 封面设计 张 楠 版式设计 杜微言
责任印制 朱学忠

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	涿州市星河印刷有限公司	网上订购	http://www.landraco.com
开 本	787mm × 1092mm 1/16		http://www.landraco.com.cn
印 张	27.25	版 次	2013年1月第1版
字 数	590千字	印 次	2013年1月第1次印刷
购书热线	010-58581118	定 价	59.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换

物料号 34471-00

“十二五”国家重点图书出版规划项目

INFORMATION SECURITY SERIES

INFORMATION SECURITY SERIES

Information Security Series systematically introduces the fundamentals of information security design and application. The goals of the Series are:

- to provide fundamental and emerging theories and techniques to stimulate more research in cryptology, algorithms, protocols, and architectures
- to inspire professionals to understand the issues behind important security problems and the ideas behind the solutions
- to give references and suggestions for additional reading and further study

Publications consist of advanced textbooks for graduate students as well as researcher and practitioner references covering the key areas, including but not limited to:

— Modern Cryptography
— Cryptographic Protocols and Network Security Protocols
— Computer Architecture and Security
— Database Security
— Multimedia Security
— Computer Forensics
— Intrusion Detection

LEAD EDITORS

EDITORIAL BOARD

ABOUT THE AUTHOR

Professor Song Y. Yan majored in both Computer Science and Mathematics, and obtained a PhD in Number Theory in the Department of Mathematics at the University of York, England. His current research interests include Computational Number Theory, Computational Complexity Theory, Algebraic Coding Theory, Public-Key Cryptography and Information/Network Security. He published, among others, the following five well-received and popular books in computational number theory and public-key cryptography:

[1] *Perfect, Amicable and Sociable Numbers: A Computational Approach*, World Scientific, 1996.

[2] *Number Theory for Computing*, Springer, First Edition, 2000, Second Edition, 2002. (Polish Translation, Polish Scientific Publishers PWN, Warsaw, 2006; Chinese Translation, Tsinghua University Press, Beijing, 2007.)

[3] *Cryptanalytic Attacks on RSA*, Springer, 2007. (Russian Translation, Moscow, 2010.)

[4] *Primality Testing and Integer Factorization in Public-Key Cryptography*, Springer, First Edition, 2004; Second Edition, 2009.

[5] *Quantum Attacks on Public-Key Cryptosystems*, Springer, 2012.

Song can be reached by email address songyuanyan@gmail.com anytime.

ACKNOWLEDGMENTS

The author would like to thank the editors at Wiley and HEP, particularly Hongying Chen, Shelley Chow, James Murphy, Clarissa Lim, and Shalini Sharma, for their encouragement, assistance, and proof-reading. Special thanks must also be given to the three anonymous referees for their very helpful and constructive comments and suggestions.

The work was supported in part by the Royal Society London, the Royal Academy of Engineering London, the Recruitment Program of Global Experts of Hubei Province, the Funding Project for Academic Human Resources Development in Institutions of Higher Learning under the Jurisdiction of the Beijing Municipality (PHR/IHLB), the Massachusetts Institute of Technology and Harvard University.

PREFACE

The book is about number theory and modern cryptography. More specically, it is about *computational* number theory and modern *public-key* cryptography based on number theory. It consists of four parts. The first part, consisting of two chapters, provides some preliminaries. Chapter 1 provides some basic concepts of number theory, computation theory, computational number theory, and modern public-key cryptography based on number theory. In chapter 2, a complete introduction to some basic concepts and results in abstract algebra and elementary number theory is given.

The second part is on computational number theory. There are three chapters in this part. Chapter 3 deals with algorithms for primality testing, with an emphasis on the Miller-Rabin test, the elliptic curve test, and the AKS test. Chapter 4 treats with algorithms for integer factorization, including the currently fastest factoring algorithm NFS (Number Field Sieve), and the elliptic curve factoring algorithm ECM (Elliptic Curve Method). Chapter 5 discusses various modern algorithms for discrete logarithms and for elliptic curve discrete logarithms. It is well-known now that primality testing can be done in polynomial-time on a digital computer, however, integer factorization and discrete logarithms still cannot be performed in polynomial-time. From a computational complexity point of view, primality testing is feasible (tractable, easy) on a digital computer, whereas integer factorization and discrete logarithms are infeasible (intractable, hard, difficult). Of course, no-one has yet been able to prove that the integer factorization and the discrete logarithm problems must be infeasible on a digital computer.

Building on the results in the first two parts, the third part of the book studies the modern cryptographic schemes and protocols whose security relies exactly on the infeasibility of the integer factorization and discrete logarithm problems. There are four chapters in this part. Chapter 6 presents some basic concepts and ideas of secret-key cryptography. Chapter 7 studies the integer factoring based public-key cryptography, including, among others, the most famous and widely used RSA cryptography, the Rabin cryptosystem, the probabilistic encryption and the zero-knowledge proof protocols. Chapter 8 studies the discrete logarithm based cryptography, including the DHM key-exchange protocol (the world's first public-key system), the ElGamal cryptosystem, and the US Government's Digital Signature Standard (DSS), Chapter 9 discusses various cryptographic systems and digital signature schemes based on the infeasibility of the elliptic curve discrete logarithm problem, some of them are just the elliptic curve analogues of the ordinary public-key cryptography such as elliptic curve DHM, elliptic curve ElGamal, elliptic curve RSA, and elliptic curve DSA/DSS.

It is interesting to note that although integer factorization and discrete logarithms cannot be solved in polynomial-time on a classical *digital* computer, they all can be solved in polynomial-time on a quantum computer, provided that a practical quantum computer with several thousand quantum bits can be built. So, the last part of the book is on quantum computational number theory and quantum-computing resistant cryptography. More speciffically, in Chapter 10, we shall study efficient quantum algorithms for solving the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP). Since IFP, DLP and ECDLP can be solved efficiently on a quantum computer, the IFP, DLP and ECDLP based cryptographic systems and protocols can be broken efficiently on a quantum computer. However, there are many infeasible problems such as the coding-based problems and the lattice-based problems that cannot be solved in polynomial-time even on a quantum computer. That is, a quantum computer is basically a special type of computing device using a different computing paradigm, it is only suitable or good for some special problems such as the IFP, DLP and ECDLP problems. Thus, in chapter 11, the last chapter of the book, we shall discuss some quantum-computing resistant cryptographic systems, including the coding-based and lattice-based cryptographic systems, that resist all known quantum attacks. Note that quantum-computing resistant cryptography is still classic cryptography, but quantum resistant. We shall, however, also introduce a truly quantum cryptographic scheme, based on ideas of quantum mechanics and some DNA cryptographic schemes based on idea of DNA molecular computation.

The materials presented in the book are based on the author's many years teaching and research experience in the field, and also based on the author's other books published in the past ten years or so, particularly the following three books, all by Springer:

[1] Number Theory for Computing, 2nd Edition, 2002.
[2] Cryptanalytic Attacks on RSA, 2007.
[3] Primality Testing and Integer Factorization in Public-Key Cryptography, 2nd Edition, 2009.

The book is suited as a text for final year undergraduate or first year postgraduate courses in computational number theory and modern cryptography, or as a basic research reference in the field.

Corrections, comments and suggestions from readers are very welcomed and can be sent via email to songyuanyan@gmail.com.

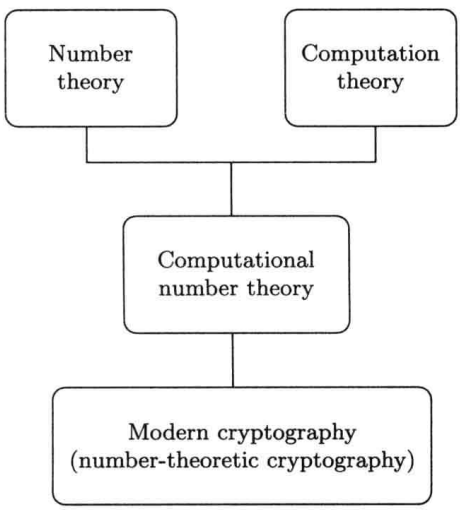
Song Y. Yan
London, England
June 2012

CONTENTS

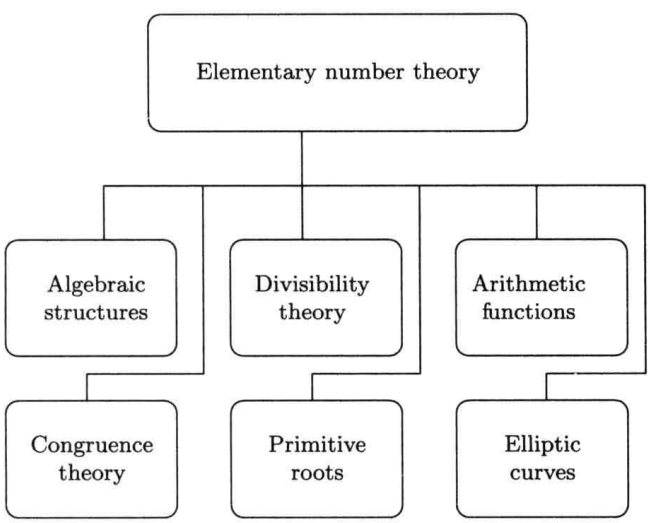
Part I

Preliminaries

In this part, we shall first explain what are number theory, computation theory, computational number theory, and modern (number-theoretic) cryptography are. The relationship betweeen them may be shown in the following figure:



Then we shall present an introduction to the elementary theory of numbers from an algebraic perspective (see the following figure), that shall be used throughout the book.



1

Introduction

In this chapter, we present some basic concepts and ideas of number theory, computation theory, computational number theory, and modern (number-theoretic) cryptography. More specifically, we shall try to answer the following typical questions in the field:

- What is number theory?
- What is computation theory?
- What is computational number theory?
- What is modern (number-theoretic) cryptography?

1.1 What is Number Theory?

Number theory is concerned mainly with the study of the properties (e.g., the divisibility) of the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

particularly the positive integers

$$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}.$$

For example, in divisibility theory, all positive integers can be classified into three classes:

1. Unit: 1.
2. Prime numbers: $2, 3, 5, 7, 11, 13, 17, 19, \cdots$.
3. Composite numbers: $4, 6, 8, 9, 10, 12, 14, 15, \cdots$.

Recall that a positive integer $n > 1$ is called a prime number, if its only divisors are 1 and n, otherwise, it is a composite number. 1 is neither prime number nor composite number. Prime numbers play a central role in number theory, as any positive integer $n > 1$ can be written uniquely into the following standard prime factorization form:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1.1}$$

Computational Number Theory and Modern Cryptography, First Edition. Song Y. Yan.

Table 1.1 $\pi(x)$ for some large x

x	$\pi(x)$
10^{15}	29844570422669
10^{16}	279238341033925
10^{17}	2623557157654233
10^{18}	24739954287740860
10^{19}	234057667276344607
10^{20}	2220819602560918840
10^{21}	21127269486018731928
10^{22}	201467286689315906290
10^{23}	1925320391606803968923
10^{24}	18435599767349200867866

where $p_1 < p_2 < \cdots < p_k$ are primes and $\alpha_1, \alpha_2, \cdots, \alpha_k$ positive integers. Although prime numbers have been studied for more than 2000 years, there are still many open problems about their distribution. Let us investigate some of the most interesting problems about prime numbers.

1. The distribution of prime numbers.
   Euclid proved 2000 years ago in his *Elements* that there were infinitely many prime numbers. That is, the sequence of prime numbers

$$2, 3, 5, 7, 11, 13, 17, 19, \cdots$$

   is endless. For example, 2, 3, 5 are the first three prime numbers, whereas $2^{43112609} - 1$ is the largest prime number to date, it has 12978189 digits and was found on 23 August 2008. Let $\pi(x)$ denote the prime numbers up to x (Table 1.1 gives some values of $\pi(x)$ for some large x), then Euclid's theorem of infinitude of primes actually says that

$$\pi(x) \to \infty, \quad \text{as } x \to \infty.$$

   A much better result about the distribution of prime numbers is the Prime Number theorem, stating that

$$\pi(x) \sim x/\log x. \tag{1.2}$$

   In other words,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1. \tag{1.3}$$

   Note that the log is the natural logarithm $\log_e$ (normally denoted by ln), where $e = 2.7182818\ldots$. However, if the Riemann Hypothesis [3] is true, then there is a refinement of the Prime Number theorem

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + \mathcal{O}\left(xe^{-c\sqrt{\log x}}\right) \tag{1.4}$$

to the effect that

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + \mathcal{O}\left(\sqrt{x}\log x\right). \tag{1.5}$$

Of course we do not know if the Riemann Hypothesis is true. Whether or not the Riemann Hypothesis is true is one of the most important open problems in mathematics, and in fact it is one of the seven Millennium Prize Problems proposed by the Clay Mathematics Institute in Boston in 2000, each with a one million US dollars prize [4]. The Riemann hypothesis states that all the nontrivial (complex) zeros ρ of the ζ function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s = \sigma + it, \quad \sigma,\ t \in \mathbb{R},\ i = \sqrt{-1} \tag{1.6}$$

lying in the critical strip $0 < \mathrm{Re}(s) < 1$ must lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$, that is, $\rho = \frac{1}{2} + it$, where ρ denotes a nontrivial zero of $\zeta(s)$. Riemann calculated the first five nontrivial zeros of $\zeta(s)$ and found that they all lie on the critical line (see Figure 1.1), he then conjectured that all the nontrivial zeros of $\zeta(s)$ are on the critical line.

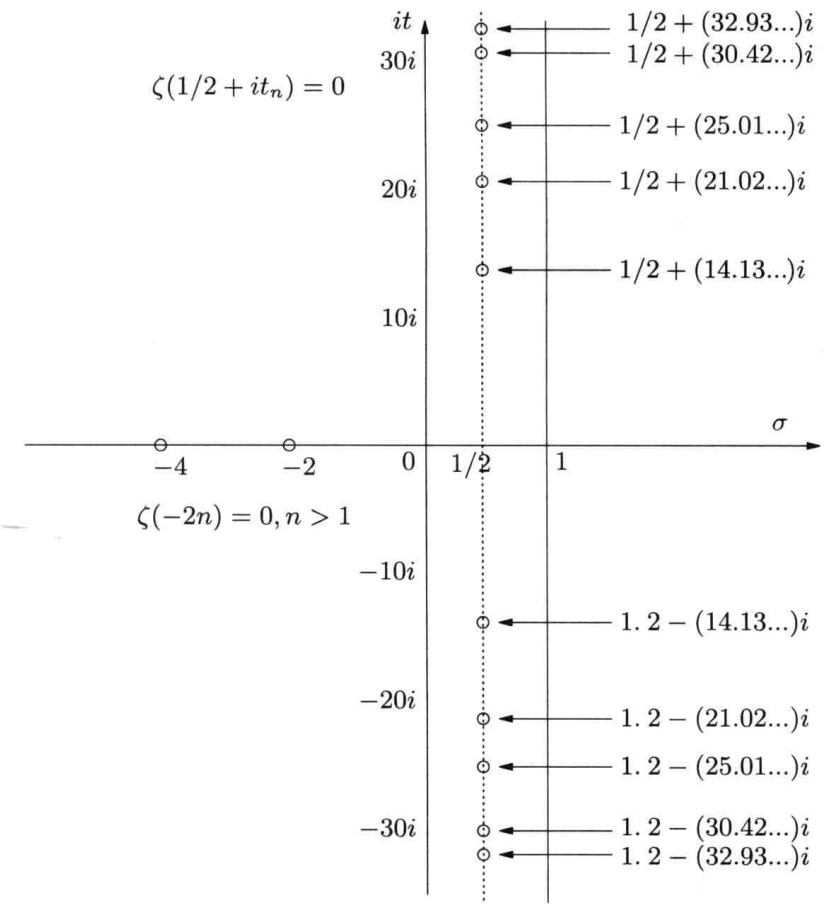


Figure 1.1 Riemann hypothesis