PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY

Advances in Information Security

Sushil Jajodia
Consulting editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers as well as developers are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

SYNCHRONIZING E-SECURITY by Godfried B. Williams; ISBN: 1-4020-7646-0
INTRUSION DETECTION IN DISTRIBUTED SYSTEMS: An Abstraction-Based Approach by Peng Ning, Sushil Jajodia and X. Sean Wang ISBN: 1-4020-7624-X
SECURE ELECTRONIC VOTING edited by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
DISSEMINATING SECURITY UPDATES AT INTERNET SCALE by Jun Li, Peter Reiher, Gerald J. Popek; ISBN: 1-4020-7305-4
SECURE ELECTRONIC VOTING by Dimitris A. Gritzalis; ISBN: 1-4020-7301-1
APPLICATIONS OF DATA MINING IN COMPUTER SECURITY, edited by Daniel Barbará, Sushil Jajodia; ISBN: 1-4020-7054-3
MOBILE COMPUTATION WITH FUNCTIONS by Zeliha Dilsun Kırlı, ISBN: 1-4020-7024-1
TRUSTED RECOVERY AND DEFENSIVE INFORMATION WARFARE by Peng Liu and Sushil Jajodia, ISBN: 0-7923-7572-6
RECENT ADVANCES IN RSA CRYPTOGRAPHY by Stefan Katzenbeisser, ISBN: 0-7923-7438-X
E-COMMERCE SECURITY AND PRIVACY by Anup K. Ghosh, ISBN: 0-7923-7399-5
INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia, ISBN: 0-7923-7204-2

Additional information about this series can be obtained from
http://www.wkap.nl/prod/s/ADIS

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY

by

Song Y. Yan
Coventry University, United Kingdom

SPRINGER SCIENCE+BUSINESS MEDIA, LLC

Library of Congress Cataloging-in-Publication

PRIMALITY TESTING AND INTEGER FACTORIZATION IN PUBLIC-KEY CRYPTOGRAPHY
by Song Y. Yan
ISBN 978-1-4757-3818-6 ISBN 978-1-4757-3816-2 (eBook)
DOI 10.1007/978-1-4757-3816-2

Printed on acid-free paper.

Dedicated to Professor Shiing-Shen Chern

for his 92nd Birthday

Preface

The problem of distinguishing prime numbers from composite, and of resolving composite numbers into their prime factors, is one of the most important and useful in all arithmetic. ... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated.

C. F. GAUSS (1777–1855)

Primality testing and integer factorization, as identified by Gauss in his *Disquisitiones Arithmeticae*, Article 329, in 1801, are the two most fundamental problems, as well as two most important research fields in number theory, particularly in *computational* number theory[1]. With the advent of digital computers, they have also been found unexpected and surprising applications in computing and particularly in cryptography and information security. In this book, we shall introduce various methods/algorithms for primality testing and integer factorization, and their applications in public-key cryptography and information security. More specifically, we shall first review some basic concepts and results in number theory in Chapter 1. Then in Chapter 2 we shall discuss various algorithms for primality testing and prime number generation, with an emphasis on the Miller-Rabin probabilistic test, the Goldwasser-Kilian and Atkin-Morain elliptic curve tests, and the Agrawal-Kayal-Saxena deterministic test. There is also an introduction to large prime number generation in Chapter 2. In Chapter 3 we shall introduce various algorithms, particularly the Elliptic Curve Method (ECM), the Quadratic Sieve (QS) and the Number Field Sieve (NFS) for integer factorization. Also in Chapter 3 we shall discuss some other computational problems that are related to factoring, such as the square root problem, the discrete logarithm problem and the quadratic residuosity problem. In Chapter 4, we shall discuss

[1] Of course, the primality testing problem (PTP) has *now* been solved, thanks to Agrawal, Kayal and Saxena [5]. That is, the PTP can now be solved in $\mathcal{P}$ (deterministic polynomial-time). However, the integer factorization problem (IFP) is still open. That is, we still do not have an efficient (i.e., deterministic polynomial-time) algorithm for IFP; in the author's opinion, the IFP may indeed be an $\mathcal{NP}$-hard problem, although no proof can be given yet at present.

some of the most widely used cryptographic systems based on the computationally intractable problems such as integer factorization, square roots, quadratic residuosity, discrete logarithms, and elliptic curve discrete logarithms.

We have tried to make this book as self-contained as possible, so that it can be used either as a textbook suitable for a course for final-year undergraduate or first-year postgraduate students, or as a basic reference in the field.

Acknowledgments

I would like to thank the three anonymous referees for their very helpful comments and kind encouragements. I would also like to thank Susan Lagerstrom-Fife and Sharon Palleschi of Kluwer Academic Publishers in Boston, and Prof. Sushil Jajodia of George Mason University, Editor of the Advances in Information Security Series, for their encouragement and help. Special thanks must be given to Dr. Bob Newman for his genius support during the preparation of this book, and to Dr. Nick Godwin for proofreading the final manuscript of the book. Finally, I would like to thank Prof. Martin Hellman, Stanford University and Prof. Shiing-Shen Chern, Director Emeritus of the Mathematical Sciences Research Institute in Berkeley for their kind encouragement and guidance.

Coventry, September 2003 S. Y. Y.

Table of Contents

Notation

All notation should be as simple as the nature of the operations to which it is applied.

CHARLES BABBAGE (1791–1871)

Notation	Explanation
$\mathbb{N}$	set of natural numbers: $\mathbb{N} = \{1, 2, 3, \cdots\}$
$\mathbb{Z}$	set of integers (whole numbers): $\mathbb{Z} = \{0, \pm n : n \in \mathbb{N}\}$
$\mathbb{Z}^+$	set of positive integers: $\mathbb{Z}^+ = \mathbb{N}$
$\mathbb{Z}_{>1}$	set of positive integers greater than 1: $\mathbb{Z}_{>1} = \{n : n \in \mathbb{Z} \text{ and } n > 1\}$
$\mathbb{Q}$	set of rational numbers: $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$
$\mathbb{R}$	set of real numbers: $\mathbb{R} = \{n + 0.d_1d_2d_3\cdots : n \in \mathbb{Z},\ d_i \in \{0, 1, \cdots, 9\}$ and no infinite sequence of 9's appears$\}$
$\mathbb{C}$	set of complex numbers: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\}$
$\mathbb{Z}/n\mathbb{Z}$	also denoted by $\mathbb{Z}_n$, residue classes modulo n; ring of integers modulo n; field if n is prime
$(\mathbb{Z}/n\mathbb{Z})^*$	multiplicative group; the elements of this group are the elements in $\mathbb{Z}/n\mathbb{Z}$ that are relatively prime to n: $(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$
$\#((\mathbb{Z}/n\mathbb{Z})^*)$	also denoted by $\lvert(\mathbb{Z}/n\mathbb{Z})^*\rvert$, order of the group $(\mathbb{Z}/n\mathbb{Z})^*$, i.e., the number of elements in the group
$\mathbb{F}_p$	finite field with p elements, where p is a prime number
$\mathbb{F}_q$	finite field with $q = p^k$ a prime power

$\mathbb{Z}[x]$	set of polynomials with integer coefficients
$\mathbb{Z}_n[x]$	set of polynomials with coefficients from $\mathbb{Z}_n$
$\mathbb{Z}[x]/h(x)$	set of polynomials modulo polynomial $h(x)$, with integer coefficients
$\mathbb{Z}_p[x]/h(x)$	also denoted by $\mathbb{F}_p[x]/h(x)$; set of polynomials modulo polynomial $h(x)$, with coefficients from $\mathbb{Z}_p$
G	group
$\|G\|$	also denoted by $\#(G)$, order of group G
R	ring
K	(arbitrary) field
E	elliptic curve $y^2 = x^3 + ax + b$
$E/\mathbb{Q}$	elliptic curve over $\mathbb{Q}$
$E/\mathbb{Z}_n$	elliptic curve over $\mathbb{Z}_n$
$E/\mathbb{F}_p$	elliptic curve over $\mathbb{F}_p$
$\mathcal{O}_E$	point at infinity on E
$E(\mathbb{Q})$	elliptic curve group formed by points on $E/\mathbb{Q}$
$\|E(\mathbb{Q})\|$	number of points in $E(\mathbb{Q})$
$\Delta(E)$	discriminant of E, $\Delta(E) = -16(4a^3 + 27b^2) \neq 0$
F_n	Fermat numbers: $F_n = 2^{2^n} + 1,\ n \geq 0$
$\mathcal{P}$	class of problems solvable in deterministic polynomial time
$\mathcal{NP}$	class of problems solvable in non-deterministic polynomial time
$\mathcal{RP}$	class of problems solvable in random polynomial time with one-sided errors
$\mathcal{ZPP}$	class of problems solvable in random polynomial time with zero errors
IFP	Integer Factorization Problem
DLP	Discrete Logarithm Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
SQRTP	SQuare RooT Problem
QRP	Quadratic Residuosity Problem
CFRAC	Continued FRACtion method (for factoring)
ECM	Elliptic Curve Method

NFS	Number Field Sieve
QS/MPQS	Quadratic Sieve/Multiple Polynomial Quadratic Sieve
ECPP	Elliptic Curve Primality Proving
DHM	Diffie-Hellman-Merkle
RSA	Rivest-Shamir-Adleman
DSA/DSS	Digital Signature Algorithm/Digital Signature Standard
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$p^\alpha \mid\mid n$	$p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$
$\gcd(a, b)$	greatest common divisor of (a, b)
$\mathrm{lcm}(a, b)$	least common multiple of (a, b)
$\lfloor x \rfloor$	floor: also denoted by $[x]$; the greatest integer less than or equal to x
$\lceil x \rceil$	ceiling: the least integer greater than or equal to x
x mod n	remainder: $x - n \left\lfloor \frac{x}{n} \right\rfloor$
$x = y \bmod n$	x is equal to y reduced to modulo n
$x \equiv y \pmod{\mathrm{n}}$	x is congruent to y modulo n
$x \not\equiv y \pmod{\mathrm{n}}$	x is not congruent to y modulo n
$f(x) \equiv g(x) \pmod{\mathrm{h(x), n}}$	$f(x)$ is congruent to $g(x)$ modulo $h(x)$, with coefficients modulo n
$[a]_n$	residue class of a modulo n
$+_n$	addition modulo n
$-_n$	subtraction modulo n
$\cdot_n$	multiplication modulo n
$\sqrt{x} \pmod{n}$	square root of x modulo n
$\sqrt[k]{x} \pmod{n}$	kth root of x modullo n
$x^k \bmod n$	x to the power k modulo n
$\log_x y \bmod n$	discrete logarithm of y to the base x modulo n
x^k	x to the power k
kP	$kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ summands}}$, where P is a point (x, y) on elliptic curve $E: \ y^2 = x^3 + ax + b$

$kP \bmod n$	kP modulo n, where P is a point on E
$\log_P Q \bmod n$	elliptic curve discrete logarithm of Q to the base P modulo n, where P and Q are points on elliptic curve E
$\mathrm{ord}_n(a)$	order of an integer a modulo n; also denoted by $\mathrm{ord}(a, n)$
$\mathrm{ind}_{g,n} a$	index of a to the base g modulo n; also denoted by $\mathrm{ind}_g a$ whenever n is fixed
$\sim$	asymptotic equality
$\approx$	approximate equality
∞	infinity
$\Longrightarrow$	implication
$\Longleftrightarrow$	equivalence
$\Box$	blank symbol; end of proof
$\sqcup$	space
Prob	probability measure
$\|S\|$	cardinality of set S
$\in$	member of
$\subset$	proper subset
$\subseteq$	subset
$\star, *$	binary operations
$\oplus$	binary operation (addition)
$\odot$	binary operation (multiplication)
$f(x) \sim g(x)$	$f(x)$ and $g(x)$ are asymptotically equal
$\perp$	undefined
$f(x)$	function of x
f^{-1}	inverse of f
$\binom{n}{i}$	binomial coefficient: $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$
$\int$	integration
$\mathrm{Li}(x)$	logarithmic integral: $\mathrm{Li}(x) = \displaystyle\int_2^x \frac{\mathrm{d}t}{\ln t}$
$\sum_{i=1}^{n} x_i$	sum: $x_1 + x_2 + \cdots + x_n$

$\prod_{i=1}^{n} x_i$	product: $x_1 x_2 \cdots x_n$
$n!$	factorial: $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$
$\log_b x$	logarithm of x to the base b ($b \neq 1$): $x = b^{\log_b x}$
$\log x$	binary logarithm: $\log_2 x$
$\ln x$	natural logarithm: $\log_e x$, $e = \sum_{n\geq 0} \frac{1}{n!} \approx 2.7182818$
$\exp(x)$	exponential of x: $e^x = \sum_{n\geq 0} \frac{x^n}{n!}$
$\pi(x)$	number of primes less than or equal to x: $\pi(x) = \sum_{\substack{p\leq x \\ p \text{ prime}}} 1$
$\tau(n)$	number of positive divisors of n: $\tau(n) = \sum_{d\mid n} 1$
$\sigma(n)$	sum of positive divisors of n: $\sigma(n) = \sum_{d\mid n} d$
$\phi(n)$	Euler's totient function: $\phi(n) = \sum_{\substack{0\leq k<n \\ \gcd(k,n)=1}} 1$
$\lambda(n)$	Carmichael's function: $\lambda(n) = \mathrm{lcm}\,(\lambda(p_1^{\alpha_1})\lambda(p_2^{\alpha_2})\cdots\lambda(p_k^{\alpha_k}))$ if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$
$\mu(n)$	Möbius function
$\zeta(s)$	Riemann zeta-function: $\zeta(s) = \prod_{n=1}^{\infty} \frac{1}{n^s}$, where s is a complex variable
$\left(\frac{a}{p}\right)$	Legendre symbol, where p is prime
$\left(\frac{a}{n}\right)$	Jacobi symbol, where n is composite
Q_n	set of all quadratic residues of n
$\overline{Q}_n$	set of all quadratic non-residues of n
J_n	$J_n = \left\{a \in (\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right) = 1\right\}$
$\tilde{Q}_n$	set of all pseudo-squares of n: $\tilde{Q}_n = J_n - Q_n$
$K(k)_n$	set of all kth power residues of n, where $k \geq 2$
$\overline{K(k)}_n$	set of all kth power non-residues of n, where $k \geq 2$
$[q_0, q_1, q_2, \cdots, q_n]$	finite simple continued fraction
$C_k = \frac{P_k}{Q_k}$	kth convergent of a continued fraction

$[q_0, q_1, q_2, \cdots]$	infinite simple continued fraction
$[q_0, q_1, \cdots, q_k, \overline{q_{k+1}, q_{k+2}, \cdots, q_{k+m}}]$	periodic simple continued fraction
e_k	encryption key
d_k	decryption key
$E_{e_k}(M)$	encryption process $C = E_{e_k}(M)$, where M is the plain-text
$D_{d_k}(C)$	decryption process $M = D_{d_k}(C)$, where C is the cipher-text
$\mathcal{O}(\cdot)$	upper bound: $f(n) = \mathcal{O}(g(n))$ if there exists *some* constant $c > 0$ such that $f(n) \leq c \cdot g(n)$
$\mathcal{O}(N^k)$	polynomial-time complexity measured in terms of arithmetic operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^k\right)$	polynomial-time complexity measured in terms of bit operations, where $k > 0$ is a constant
$\mathcal{O}\left((\log N)^{c \log N}\right)$	superpolynomial complexity, where $c > 0$ is a constant
$\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right)$	subexponential complexity, $\mathcal{O}\left(\exp\left(c\sqrt{\log N \log\log N}\ \right)\right) = \mathcal{O}\left(N^{c\sqrt{\log\log N/\log N}}\right)$
$\mathcal{O}\left(\exp(x)\right)$	exponential complexity, sometimes denoted by $\mathcal{O}\left(e^x\right)$
$\mathcal{O}\left(N^\epsilon\right)$	exponential complexity measured in terms of bit operations; $\mathcal{O}\left(N^\epsilon\right) = \mathcal{O}\left(2^{\epsilon \log N}\right)$, where $\epsilon > 0$ is a constant