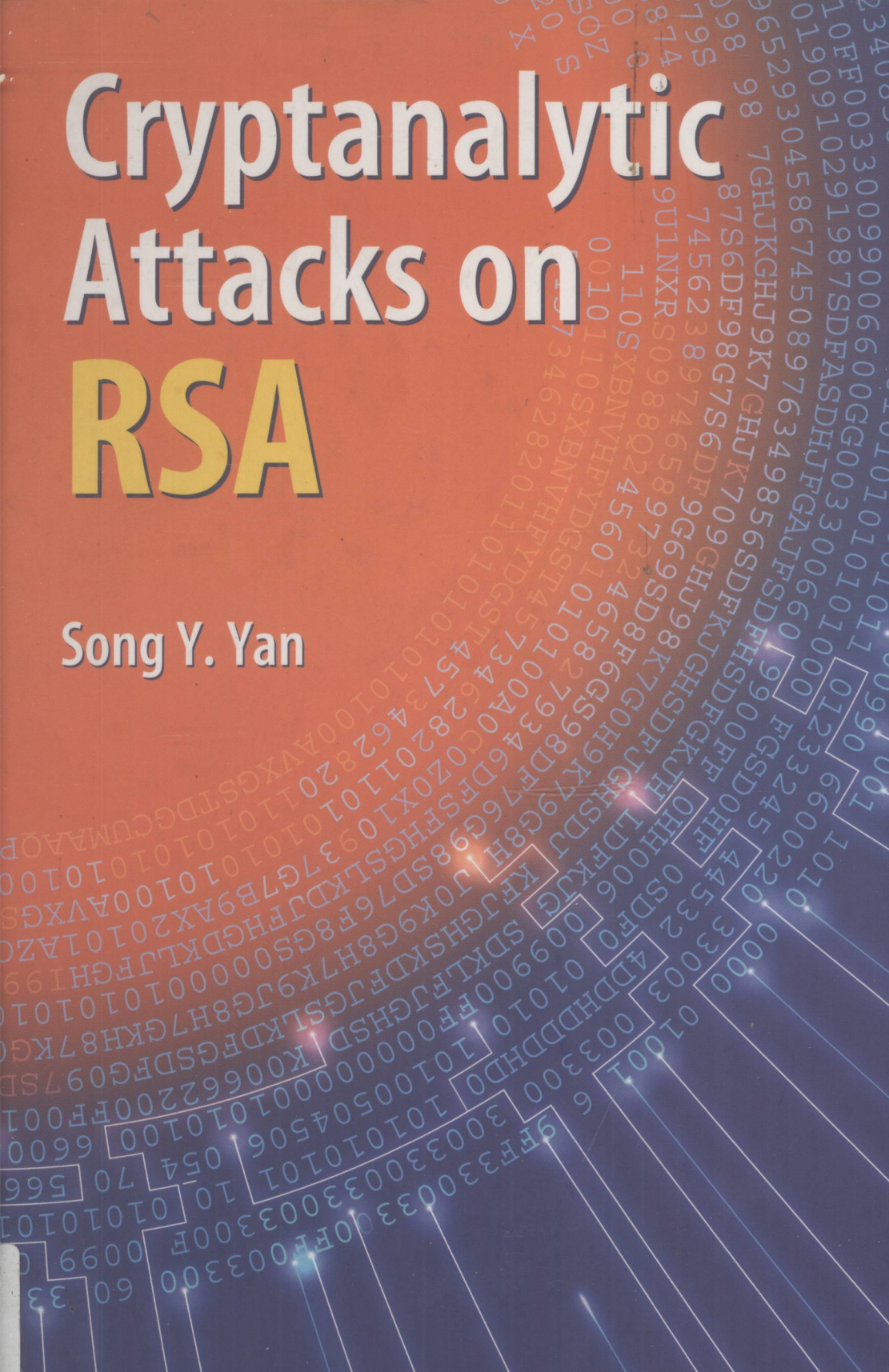
Cryptanalytic Attacks on RSA

Song Y. Yan



Cryptanalytic Attacks on RSA

by

Song Y. Yan
University of Bedfordshire, UK
and
Massachusetts Institute of Technology, USA

Springer

Song Y. Yan, PhD
Professor of Computer Science and Mathematics
Director, Institute for Research in Applicable
Computing
University of Bedfordshire
Bedfordshire LU1 3JU
UK
song.yan@beds.ac.uk
and
Visiting Professor
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139-4307
USA
syan@math.mit.edu

ISBN-13: 978-0-387-48741-0 e-ISBN-13: 978-0-387-48742-7

Library of Congress Control Number: 2007934650

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

Cryptanalytic Attacks on RSA

Dedicated to Professor Glyn James
on the occasion of his 70th birthday
with gratitude for his encouragement and support

Preface

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

SUN TZU
The Art of War (500 BC)

The book is about the cryptanalytic attacks on RSA. RSA is the first *workable* and *practical* public-key cryptographic system, invented in 1977 and published in 1978, by Rivest, Shamir and Adleman, then all at the Massachusetts Institute of Technology (MIT), and is still the most widely used cryptographic systems in e.g., online transactions, emails, smartcards, and more generally electronic and mobile commerce over the Internet, for which its three inventors received the year 2002 Turing Award, a prize considered to be the equivalent *Nobel Prize for Computer Science*. The security of RSA relies on the computational intractability of the Integer Factorization Problem (IFP), for which, no efficient (i.e., polynomial-time) algorithm is known. To get an idea how difficult the *integer factorization* is, let us consider the following 2048 bits (617 digits) composite number, known as RSA-2048:

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357.

It is a *product* of two *prime numbers*. The RSA Data Security Incorporation currently offers a $200,000 prize for the first person or group finding

its two prime factors. The basic idea of RSA encryption and decryption is, surprisingly, rather simple:

$$C \equiv M^e \pmod{N}, \quad M \equiv C^d \pmod{N},$$

where $N = pq$ with p and q prime, M, C, e and d are the plaintext, ciphertext, encryption exponent and decryption exponent, respectively. Note that e and d must be satisfied with the condition that $ed \equiv 1 \pmod{\phi(N)}$, where $\phi(N) = (p-1)(q-1)$ is Euler's ϕ-function. Let, for example, $e = 65537$, N be the above mentioned number RSA-2048, and C the following number:

$$\begin{aligned}
&218598056144555493024019389629177159753811144728543422921500499254_\\
&181211032562087679022259831067991286101190897695119357754765408522_\\
&697956638242922870637083231694404873947694078432775781998614979942_\\
&064361669462614088852741600217233052059574880668463536030287944235_\\
&822627708134997061064700771693064600712629809165416998449992925313_\\
&374281387325903328781863209595468701560742767599157207314869432305_\\
&892651836189508103764678721683360183118994273706398707795480800698_\\
&501878875875150532123738006235671958527639461339868604410378449818_\\
&383913059864587128396200112815989134558427750667427151537609736712_\\
&0464775711605903168458 7.
\end{aligned}$$

To recover M from C one requires to find d; to find d one needs to calculate $\phi(N)$; to calculate $\phi(N)$ one needs to factor N. But unfortunately, factorizing N is intractable when N is large (in the present case, N is a 2048-bit number, which is far beyond the computing power of any factoring algorithm on any computer at present); no polynomial-time factoring algorithm is known so far. Thus, RSA is secure and C is safe since it is difficult to recover M from C without factoring N. This is essentially the whole idea of RSA! One can try to decrypt the above given RSA ciphertext C or try to factor the number RSA-2048 in order to get an idea how difficult it is to break RSA or to factor a large number.

The book consists of ten chapters. Chapter 1 presents some computational and mathematical preliminaries, particularly the theory and practice of tractable and intractable computations in number theory. Chapter 2 introduces the basic concepts and theory of the RSA cryptographic system and its variants in a broad sense. As the security of RSA is based on the intractability of the Integer Factorization Problem (IFP), which is also closely related to the Discrete Logarithm Problem (DLP), the attacks based on solutions to IFP problem are discussed in Chapter 3, whereas the attacks based on solutions to DLP problem are discussed in Chapter 4. As quantum algorithm is applicable to both the IFP problem and the DLP problem, Chapter 5 will discuss some quantum attacks on RSA via quantum order finding, quantum factoring and quantum discrete logarithm solving. Chapter 6 concentrates on some simple elementary number-theoretic attacks on RSA, including e.g., forward attack, short plaintext attack, common modulus attack and fixed-point

attack. It is common that to speed-up the computation of RSA encryption, a short public exponent e is often used. It is also true for the RSA decryption if a short private exponent d is used. However, the use of short exponent e or d can be dangerous. So, in Chapter 7 we shall discuss some cryptanalytic attacks on the short RSA public exponent e, whereas in Chapter 8 we shall discuss some attacks on the short RSA private exponent d. In Chapter 9, a completely different type of attacks, namely, the side-channel attacks on RSA, are discussed. Unlike the mathematical/algorithmic attacks in the previous chapters, side-channel attacks do not exploit the mathematical properties or weakness of the RSA algorithm/system itself, but exploit the hardware implementation issues of the system. In other words, these attacks are nothing to do with the RSA algorithm/system itself but have something to do with the hardware implementation of the RSA algorithm/system. Chapter 10, the final chapter, presents some quantum resistant, non-factoring based cryptographic systems as an alternative/replacement to RSA, such as lattice based and code-based cryptosystems, so that once RSA is proved to be insecure, there is an immediate replacement to the insecure RSA.

The book is self-contained and the materials presented in the book have been extensively classroom tested for various courses in Cryptography and Cryptanalysis at Aston and Coventry Universities in England, and the South China University of Technology and Nankai University in China. Many parts of the materials in the book have also been presented in seminars in various universities around the world. Hence, the book is suitable *either* as a research reference for public-key cryptology in general and for RSA cryptology in particular, *or* as a graduate text in the field.

Acknowledgments

The author would like to thank Prof Sushil Jajodia of George Mason University, USA, Prof Glyn James and Dr Anne James of Coventry University, UK, Prof Stephen Cook of the University of Toronto, Canada, and Prof Richard Brent of Oxford University and Australian National University for their encouragement, support and help during the writing of the book. Special thanks must also be given to Susan Lagerstrom-Fife and Sharon Palleschi, the editors at Springer in Boston, USA, for their encouragement, support and help.

Parts of book were written while the author visited the following three places: the Department of Computer Science at the University of Toronto (UT) in March-April 2005, hosted by Prof Stephen Cook and supported by UT and the Royal Society London, the Mathematical Science Institute at the Australian National University (ANU) in October-November 2006, hosted by Prof Richard Brent and supported by ANU and the Royal Society London,

and the Department of Mathematics at the Massachusetts Institute of Technology (MIT) in July-Sept 2007, hosted by Prof Michael Sipser and supported by MIT.

Special thanks must also be given to Prof Glyn James at Coventry University and Prof Richard Brent at Oxford University and Australian National University for reading the whole manuscript of the book, to Prof Brain Scotney at Ulster University for his constant encouragement during the writing of the book, and to Prof Michael Sipser for inviting me to visit and work at MIT where the book was finally completed.

The struggle between code-makers and code-breakers is endless. The struggle between attacks and anti-attacks on RSA is also endless as soon as RSA is till in use. New ideas and new attacks on RSA may be conceived and invented anytime. So comments, corrections and suggestions on the book, and new ideas and news attacks on RSA are particularly very welcome from the readers, and can be sent to any one of my following three email addresses: song.yan@beds.ac.uk, syan@math.mit.edu, or syan@cs.toronto.edu, so that I can incorporate them into a future edition of the book. Thank you for your help in advance.

CAMBRIDGE, MASSACHUSETTS, AUGUST 2007 S. Y. Y.

Notation

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

CHARLES BABBAGE (1791–1871)
English Mathematician, Philosopher, Mechanical Engineer and Proto-Computer Scientist

Notation	**Explanation**
$\mathbb{N}$ or $\mathbb{Z}^+$	Set of natural numbers or positive integers: $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \cdots\}$
$\mathbb{Z}$	Set of integers: $\mathbb{Z} = \{0, \pm n : n \in \mathbb{N}\}$
$\mathbb{Z}_{>1}$	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: $\mathbb{R} = \{n + 0.d_1d_2d_3\cdots : n \in \mathbb{Z},\ d_i \in \{0, 1, 2, \cdots, 9\}$ and no infinite sequence of 9's appears$\}$
$\mathbb{C}$	Set of complex numbers: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}\}$
$\mathbb{Z}_N$ or $\mathbb{Z}/N\mathbb{Z}$	Residue classes modulo N: $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z} = \{0, 1, 2, \cdots, N-1\}$. Ring of integers. Field if N is prime
$\mathbb{Z}_N[x]$	Set (ring) of polynomials with integer coefficients, modulo N
$\mathbb{Z}[x]$	Set (ring) of polynomials with integer coefficients

$\mathbb{Z}_N^*$	Multiplicative group: $\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \ \gcd(a, N) = 1\}$.
$\#(\mathbb{Z}_N^*)$ or $\lvert\mathbb{Z}_N^*\rvert$	Order of the multiplicative group
$\mathbb{F}_p$ or $\mathbb{Z}_p$	Finite field with p elements, where p is a prime
$\mathbb{F}_q$	Finite field with $q = p^k$ a prime power
$f(x)$	Function of x
f^{-1}	Inverse of f
$f(x) \sim g(x)$	$f(x)$ and $g(x)$ are asymptotically equal
$\binom{n}{i}$	Binomial coefficient: $\binom{n}{i} = \frac{n(n-1)(n-2)\cdots(n-i+1)}{i!}$
$\int$	Integration
$\mathrm{Li}(x)$	Logarithmic integral: $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$
$\sum_{i=1}^{n} x_i$	Sum: $x_1 + x_2 + \cdots + x_n$
$\prod_{i=1}^{n} x_i$	Product: $x_1 x_2 \cdots x_n$
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 an elliptic curve $E: \ y^2 = x^3 + ax + b$
$\mathcal{O}_E$	Point at infinity on an elliptic curve E
$\log_b x$	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: $e^x = \sum_{n \geq 0} \frac{x^n}{n!}$
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\gcd(a, b)$	Greatest common divisor of (a, b)
$\mathrm{lcm}(a, b)$	Least common multiple of (a, b)
$\lfloor x \rfloor$ or $[x]$	Greatest integer less than or equal to x
$\lceil x \rceil$	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
$x^k \bmod N$	x to the power k modulo N
$kP \bmod N$	kP modulo N, with P a point on elliptic curve E
$\mathrm{ord}_N(a)$	Order of an integer a modulo N; also denoted by $\mathrm{order}(a, N)$
$\mathrm{ind}_{g,N}(a)$	Index of a to the base g modulo N
$\log_g a \bmod N$	Discrete logarithm of a to the base g modulo N: $\log_g a \bmod N = \mathrm{ind}_{g,N}(a)$
$\pi(x)$	Prime counting function: $\pi(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} 1$
$\tau(N)$	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: $\phi(N) = \sum_{\substack{0 \le k < N \\ \gcd(k,N)=1}} 1$
$\lambda(N)$	Carmichael's function: $\lambda(N) = \mathrm{lcm}\left(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \cdots, \lambda(p_k^{\alpha_k})\right)$ if $N = \prod_{i=1}^{k} p_i^{\alpha_i}$
$\zeta(s)$	Riemann zeta-function: $\zeta(s) = \prod_{n=1}^{\infty} n^{-s}$, where $s = \sigma + it$, with $\sigma, t \in \mathbb{R}$ and $i = \sqrt{-1}$
$\left(\frac{a}{p}\right)$	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 nonresidues of N
J_N	$J_N = \left\{a \in \mathbb{Z}_N^* : \left(\frac{a}{N}\right) = 1\right\}$
$\tilde{Q}_N$	Set of all pseudosquares of N: $\tilde{Q}_N = J_N - Q_N$
$\sim$	Asymptotic equality
$\approx$	Approximate equality
∞	Infinity

$\Longrightarrow$	Implication
$\Longleftrightarrow$	Equivalence
$\square$	Blank symbol; end of proof
$\sqcup$	Space
Prob	Probability measure
$\in$	Member of
$\subset$	Proper subset
$\subseteq$	Subset
$[q_0, q_1, q_2, \cdots, q_n]$	Finite simple continued fraction: $q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots q_{n-1} + \cfrac{1}{q_n}}}}$
$[q_0, q_1, q_2, q_3, \cdots]$	Infinite simple continued fraction: $q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}}$
$C_k = \frac{P_k}{Q_k}$	k-th convergent of a continued fraction
$\mathcal{P}$	Class of problems solvable in polynomial-time by a deterministic Turing machine
$\mathcal{NP}$	Class of problems solvable in polynomial-time by a nondeterministic Turing machine
$\mathcal{ZPP}$	Class of problems solvable in polynomial-time by a random Turing machine with zero errors
$\mathcal{RP}$	Class of problems solvable in polynomial-time by a random Turing machine with one-sided errors
$\mathcal{BPP}$	Class of problems solvable in in polynomial-time by a random Turing machine with two-sided errors
co-$\mathcal{RP}$	$\mathcal{RP}$-complete problems
co-$\mathcal{NP}$	$\mathcal{NP}$-complete problems
$\mathcal{PS}$	$\mathcal{P}$ $\mathcal{S}$pace problems
$\mathcal{NPS}$	$\mathcal{NP}$ $\mathcal{S}$pace problems
CFRAC	Continued FRACtion method (for factoring)
ECM	Elliptic Curve Method (for factoring)

NFS	Number Field Sieve (for factoring)
QS/MPQS	Quadratic Sieve/Multiple Polynomial Quadratic Sieve (for factoring)
ECPP	Elliptic Curve Primality Proving
DES	Data Encryption Standard
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DHM	Diffie-Hellman-Merkle key-exchange
RSA	Rivest-Shamir-Adleman Encryption
RSAP	RSA Problem
IFP	Integer Factorization Problem
DLP	Discrete Logarithm Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
QRP	Quadratic Residuosity Problem
SQRTP	Modular Square Root Problem
RFP	k-th Root Finding Problem
LLL	Lenstra-Lenstra-Lovasz lattice reduction algorithm
SVP	Shortest Vector Problem
PNT	Prime Number Theory: $\pi(x) \sim x/\ln x$
WWW	World Wide Web
$\mathcal{M}$	Plaintext space
M	$M \in \mathcal{M}$ Plaintext
$\mathcal{C}$	Ciphertext space
C	$C \in \mathcal{C}$ Ciphertext
e_k	Encryption key
d_k	Decryption key
$E_{e_k}(M)$	Encryption $C = E_{e_k}(M)$
$D_{d_k}(C)$	Decryption $M = D_{d_k}(C)$
e	RSA encryption exponent
d	RSA decryption exponent
$E_e(M)$	RSA encryption $C = E_e(M) \equiv M^e \pmod{N}$
$D_d(C)$	RSA decryption $M = D_d(C) \equiv C^d \pmod{N}$
$M \mapsto M^e \bmod N$	RSA function

原书缺页

Table of Contents