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:

25195084756578934940271832400483985714292821262040320277771378360_436620207075955562640185258807844069182906412495150821892985591491_761845028084891200728449926873928072877767359714183472702618963750_1497182469116507761337985900973304597488084284017974291006424_5869181719511874612151517265463228221268699875491824224336372590851_41865462043576798423387184774479207399342365848238242811981638150_10674810451660377306056201619676256133844143603839044149526344321_9011465754444541784240209246165157233507787077498171257724679629263_863563732899121548314381678998850404453640235273819513786365643912_12010397122822120720357.

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 \( \phi \)-function. Let, for example, \( e = 65537 \), \( N \) be the above mentioned number RSA-2048, and \( C \) the following number:

\[
218598056144555493024019389629177159753811144728543422921500499254_{-18x676}\n181211032562087679022259831067991286101190897695119357754765408522_{-18x676}\n697956638242922870637083231694404873947694078432775781998614979942_{-06x436}\n06436166946261408885274160021723305205957488066846353603028794425_{-38x362}\n374281387325903328781863209595468701560742767599157207314869432305_{-89x265}\n8926518361895081037646787216833601831189942730763987795480800698_{-50x187}\n501878875875150532123738006235671958527639461339868604410378449818_{-38x391}\n305864587812396200112815989134558427750667427151537609736712_{-04x477}\n57116059031684587.
\]

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.
Cryptanalytic Attacks on RSA
Yan, S.Y.
2008, XX, 255 p. 20 illus., Hardcover
ISBN: 978-0-387-48741-0