ADVANCES IN INFORMATION SECURITY

Recent Advances in RSA Cryptography

Stefan Katzenbeisser

Kluwer Academic Publishers

Recent Advances in RSA Cryptography

Recent Advances in RSA Cryptography surveys the most important achievements of the last 22 years of research in RSA cryptography. Special emphasis is laid on the description and analysis of proposed attacks against the RSA cryptosystem. The first chapters introduce the necessary background information on number theory, complexity and public key cryptography. Subsequent chapters review factorization algorithms and specific properties that make RSA attractive for cryptographers. Most recent attacks against RSA are discussed in the third part of the book (among them attacks against low-exponent RSA, Hastad's broadcast attack, and Franklin-Reiter attacks). Finally, the last chapter reviews the use of the RSA function in signature schemes.

Recent Advances in RSA Cryptography is of interest to graduate level students and researchers who will gain an insight into current research topics in the field and an overview of recent results in a unified way.

Recent Advances in RSA Cryptography is suitable as a secondary text for a graduate level course, and as a reference for researchers and practitioners in industry.

ISBN 0-7923-7438-X

9 780792 374381

ADIS 3
0-7923-7438-X

Kluwer Academic Publishers

RECENT ADVANCES IN RSA CRYPTOGRAPHY

ADVANCES IN INFORMATION SECURITY

Additional titles in the series:

INFORMATION HIDING: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, and Sushil Jajodia
ISBN: 0-7923-7204-2

RECENT ADVANCES IN E-COMMERCE SECURITY AND PRIVACY by Anup K. Ghosh, *ISBN: 0-7923-7399-5*

Dedicated to Prof. Hans Kaiser, who raised my interest in mathematics.

RECENT ADVANCES IN RSA CRYPTOGRAPHY

by

Stefan Katzenbeisser
Vienna University of Technology, Austria

KLUWER ACADEMIC PUBLISHERS
Boston / Dordrecht / London

Distributors for North, Central and South America:
Kluwer Academic Publishers
101 Philip Drive
Assinippi Park
Norwell, Massachusetts 02061 USA
Telephone (781) 871-6600
Fax (781) 871-6528
E-Mail <kluwer@wkap.com>

Distributors for all other countries:
Kluwer Academic Publishers Group
Distribution Centre
Post Office Box 322
3300 AH Dordrecht, THE NETHERLANDS
Telephone 31 78 6392 392
Fax 31 78 6546 474
E-Mail <services@wkap.nl>

 Electronic Services <http://www.wkap.nl>

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available
from the Library of Congress.

Printed on acid-free paper.

Printed in the United States of America

The Publisher offers discounts on this book for course use and bulk purchases.
For further information, send email to <lance.wobus@wkap.com>

Series Foreword
ADVANCES IN INFORMATION SECURITY

Sushil Jajodia
Consulting Editor

Department of Information & Software Engineering
George Mason University
Fairfax, VA 22030-4444, U.S.A.

email: jajodia@gmu.edu

Welcome to the third volume of the Kluwer International Series on ADVANCES IN INFORMATION SECURITY. The goals of this series 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.

The success of this series depends on contributions by researchers and developers such as yourself. If you have an idea for a book that is appropriate for this series, I encourage you to contact either the Acquisitions Editor for the series, Lance Wobus (lwobus@wkap.com), or myself, the Consulting Editor for the series (jajodia@gmu.edu). We would be happy to discuss any potential projects with you. Additional information about this series can be obtained from www.wkap.nl/series.htm/ADIS.

About this volume

The third volume of this series is entitled *Recent Advances in RSA Cryptography* by Stefan Katzenbeisser. Named after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman, RSA is the best known and most important public key cryptosystem. It can be used to provide secrecy as well as digital signatures, and has become a de facto standard for implementations that use public key cryptography.

Since its publication in 1978, RSA has undergone extensive scrutiny by a number of cryptanalysts. This volume provides an excellent and up-to-date description of these fascinating efforts. The necessary background material from number theory and computational complexity is included. This volume is an essential resource for researchers as well as practitioners working in the area of security.

Stefan Katzenbeisser studied Computer Science at the Vienna University of Technology and is an editor of *Information Hiding Techniques for Steganography and Digital Watermarking* (Artech House, 2000).

SUSHIL JAJODIA
Consulting Editor

Preface

If we take in our hand any volume; of divinity or school metaphysics, for instance; let us ask, 'Does it contain any abstract reasoning concerning quantity or number?' No. 'Does it contain any experimental reasoning concerning matter of fact and existence?' No. Commit it then to the flames: for it can contain nothing but sophistry and illusion.

—David Hume

In the mid 1990's, a series of letter bomb attacks, motivated by racist reasons, struck Austria. The recipients of these bombs were people engaged in multicultural activities or who were known as supporters of refugee organizations. Several people were injured seriously. Some months later the perpetrator sent a letter of confession to the Austrian authorities, encrypted in the RSA system using the RSA modulus

$$
\begin{aligned}
n = \; & 6305482150701295471567183324958896322344341454119712758 8 \\
& 8376987603260225252787926135276738944105689100036295535 8 \\
& 6814142438653640364957870769912818949143213863190059077 4 \\
& 7292149900153691027609648847763448497178114843095289150 4 \\
& 0117952098061886881.
\end{aligned}
$$

The author(s) believed that the factorization of n would require tremendous efforts, even on a modern supercomputer, and (perhaps) speculated that their letter would be safe for a long period of time. In a cynical statement they mentioned that supercomputers were built for solving this academic, simple-looking "Highschool"-like problem. However, n can be factored immediately on a conventional PC revealing the secret factors

$$
\begin{aligned}
p = \; & 2511071912690135497619093339586712468024080571127684488 6 \\
& 2509598241562051889494061847352957883875611351675294302 4 \\
& 3075948799
\end{aligned}
$$

and

$$q = \begin{array}{l} 25110719126901354976190933395867124680240805711276844886 \\ 25095982415620518894940618473529578838756113516752943511 \\ 8429780319. \end{array}$$

Consequently, the letter of confession could be read by the authorities within some weeks. Does this incident allow to draw the conclusion that the RSA system as a whole is insecure? As RSA is perhaps one of the most frequently used public key cryptosystems, this would have enormous consequences. Luckily, the authors of the letter simply chose an instance of the RSA cryptosystem that can be broken easily (basically they made the vital mistake to choose primes p and q with only a small difference; however, it is interesting to note that both p and q are "doubly safe primes" in the sense of the definition on page 70).

Ever since the RSA cryptosystem was published in 1978 by Rivest, Shamir and Adleman, it has attracted numerous researchers with various backgrounds (number theorists, complexity theorists and computer security experts to name but a few) because of its elegance and practicability. RSA is perhaps today the most well-known public key cryptosystem; accordingly, many theoretical results regarding the security of RSA are known. Many of them are "bad news" for a cryptanalyst, stating that breaking RSA is still likely to be intractable; however, some weaknesses have been found recently in special instances of the RSA system.

This work tries to survey the most important achievements of the last 22 years of research in a unified way; special emphasis is laid on the description and analysis of proposed attacks against the RSA system. It was my goal to briefly discuss results from various aspects of RSA cryptography, but I am aware of the fact that such an effort will always remain incomplete. Due to space constraints and in order to improve understanding, some proofs are not presented in full length; in these cases only a proof sketch omitting technical details is given. If more information is needed, I refer to the literature where appropriate.

Chapters 1 and 2 introduce the necessary background information on number theory and computational complexity. Especially we need precise definitions of "efficient computation" and "computational equivalence"; the latter term will be defined using so-called reductions between computational problems. Although this monograph is not intended to be self-contained, all necessary numbertheoretic results are presented (mostly without proofs).

Chapter 3 introduces public-key cryptography, especially the RSA system. Additionally, "one-way functions," which form the basis of public-key cryptosystems, are defined and results regarding their existence are proved. The chapter concludes with a discussion of the computational complexity of (low exponent) RSA. Chapter 4 surveys the most important factorization techniques

and Chapter 5 summarizes the main properties of the RSA system that make it attractive for cryptographers. We will e.g. show that computing the decryption exponent or even the least significant bit of the plaintext, given only the public key and corresponding ciphertext, is computationally equivalent to breaking RSA as a whole.

Chapter 6 focusses on special instances of the RSA systems, namely those that use either a low encryption or decryption exponent. It will be shown that these systems are probably insecure (but we should note that all these attacks cannot be generalized to other RSA instances, so they pose no threat to the "entire" system). Chapter 7 discusses implementation and protocol attacks; attacks that do not attempt to find a "mathematical solution" to the RSA problem but rather try to find flaws in communication protocols or faulty implementations. Finally, Chapter 8 will outline possible applications of the RSA function in signature schemes.

Acknowledgements. I am grateful to all persons who read preliminary versions of this monograph and provided me with feedback, especially the anonymous referees who suggested to insert additional material for the sake of completeness. I also thank Prof. Hans Kaiser and Prof. Hans Stetter for their mathematical advices. Finally, I thank Lance Wobus and Sharon Palleschi from Kluwer for mastering all difficulties which arose during the production of this book.

The quotations appearing at the beginning of each chapter are taken from a collection of mathematical quotes maintained by Mark R. Woodard, available at `http://math.furman.edu/~mwoodard/mqs/mquot.shtml`. I am grateful for his permission to use them in this book.

Stefan Katzenbeisser

Vienna, April 2001

Contents

Foreword ix
Preface xi

1. MATHEMATICAL BACKGROUND 1
   1.1 Divisibility and the residue class ring $\mathbb{Z}_n$ 1
   1.2 Polynomials 5
   1.3 Euler's totient function and $\mathbb{Z}_n^*$ 6
   1.4 Polynomial congruences and systems of linear congruences 9
   1.5 Quadratic residues 10

2. COMPUTATIONAL COMPLEXITY 13
   2.1 Turing machines 13
   2.2 Deterministic and nondeterministic machines 14
   2.3 Decision problems and complexity classes 16
   2.4 Reductions, completeness and oracle computations 19
   2.5 **co−NP** 21
   2.6 Efficient computation and randomized complexity classes 22

3. PUBLIC KEY CRYPTOGRAPHY 25
   3.1 Public key cryptography 25
   3.2 Permutation polynomials and RSA-type cryptosystems 28
   3.3 Efficient implementation of RSA 30
   3.4 One-way functions 33
   3.5 On the complexity of an attack against RSA 41

4. FACTORIZATION METHODS 49
   4.1 Trial division and Fermat factorization 49
   4.2 Monte-carlo factorization 50
   4.3 Factor base methods 52
   4.4 The continued fraction method 54
   4.5 Quadratic sieve 57
   4.6 Other Factorization Methods 59

5. PROPERTIES OF THE RSA CRYPTOSYSTEM 63
5.1 Computing the decryption exponent 63
5.2 Partial decryption 67
5.3 Cycling attacks and superencryption 68
5.4 Incorrect keys 71
5.5 Partial information on RSA and hard-core predicates 73

6. LOW-EXPONENT RSA 81
6.1 Wiener's attack 81
6.2 Lattice basis reduction 82
6.3 The attack of Boneh and Durfee 86
6.4 Low public exponents 91
6.5 Polynomially related messages 93
6.6 Partial key exposure 96

7. PROTOCOL AND IMPLEMENTATION ATTACKS 99
7.1 Simple protocol attacks against RSA 99
7.2 Håstad's broadcast attack 102
7.3 Effective security of small RSA messages 103
7.4 Optimal Asymmetric Encryption 104
7.5 Faulty encryption 106
7.6 Timing attacks 108

8. RSA SIGNATURES 111
8.1 Attacks on RSA signatures with redundancy 111
8.2 Security of hash-and-sign signatures 115
8.3 Provably secure RSA signatures 118
8.4 Undeniable signatures 122
8.5 Threshold signatures 125

References 129

Index 137

Chapter 1

MATHEMATICAL BACKGROUND

... in mathematics you don't understand things, you just get used to them.
—John von Neumann

The aim of this chapter is to summarize important results from number theory and algebra which will be used in subsequent chapters. Most theorems are provided without proof, since their proofs can be found in many elementary text-books on number theory [47] or algebra (a proof will only be presented in case the proof technique is relevant for later applications).

1.1. Divisibility and the residue class ring $\mathbb{Z}_n$

Given two integers a and b, we say a *divides* b (and write $a \mid b$) if there exists an integer c such that $ac = b$. A divisor of 1 is called *unit* (in $\mathbb{Z}$ the only units are -1 and 1). It is easy to verify the following properties for all $a, b, c \in \mathbb{Z}$:

- $1 \mid a$ and $a \mid a$,
- from $a \mid b$ and $b \mid c$ it follows that $a \mid c$,
- if $a \mid b$ and $b \mid a$ then $a = \pm b$,
- if $a \mid b$ then $ac \mid bc$,
- if $a \mid b$ and $a \mid c$ then $a \mid (xb + yc)$ for all $x, y \in \mathbb{Z}$.

We call two elements a and b of a commutative ring with 1 associated, if there exists a unit e such that $a = eb$. A common divisor d of a and b is called *greatest common divisor*, written $d = \gcd(a, b)$, if every common divisor t of a and b divides d, i.e. if for all $t \in \mathbb{Z}$ with $t \mid a$ and $t \mid b$ we have $t \mid d$.

The greatest common divisor is unique up to multiplication with a unit; if we speak of "the gcd" in $\mathbb{Z}$, we refer to the positive greatest common divisor. The greatest common divisor of two integers can be found using one of the oldest known algorithms, the *Euclidean algorithm*, which is based on the following observation:

THEOREM 1.1 *Given two integers a and b with $b \neq 0$, we can find integers q and r with $0 \leq r < |b|$ so that $a = qb + r$.*

In the previous theorem, q can be thought of as the integer part and r as the remainder of the division a/b. Since $\gcd(a, b) = \gcd(b, a)$, $\gcd(|a|, |b|) = \gcd(a, b)$ and $\gcd(a, 0) = |a|$ it suffices to discuss the case $a \geq b > 0$. The Euclidean algorithm starts by finding—according to the previous theorem—two integers q_1 and r_1 with $a = q_1 b + r_1$ and $0 \leq r_1 < b$. Next, we can take the numbers b and r_1 as a basis for these computations, yielding two integers q_2 and r_2 with $b = q_2 r_1 + r_2$ and $0 \leq r_2 < r_1$. By iterating this step, we get the schema

$$\begin{aligned}
a &= q_1 b + r_1 && \text{with} \quad 0 \leq r_1 < b, \\
b &= q_2 r_1 + r_2 && \text{with} \quad 0 \leq r_2 < r_1, \\
r_1 &= q_3 r_2 + r_3 && \text{with} \quad 0 \leq r_3 < r_2, \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && \text{with} \quad 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}$$

The last nonzero remainder r_n is the greatest common divisor of a and b; such a remainder must exist, since the sequence r_i is strictly decreasing (i.e. $0 \leq \ldots < r_i < r_{i-1} < \ldots < r_1$). It is easy to see that r_n is a divisor of a and b by reading the schema "backwards": by observing $r_n \mid r_{n-1}$ and $r_{n-2} = q_n r_{n-1} + r_n$ we obtain $r_n \mid r_{n-2}$. Similarly, since $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$ and $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$, it follows that $r_n \mid r_{n-3}$. This argument can be applied recursively to verify that $r_n \mid a$ and $r_n \mid b$. To see that r_n is indeed a greatest common divisor of a and b, we note that for every divisor t of a and b, $t \mid a$ and $t \mid b$. From the first line of the scheme we get $t \mid r_1$ and—using this result—from the second line $t \mid r_2$. By induction, we conclude that $t \mid r_i$ for all $1 \leq i \leq n$ and thus r_n is the greatest common divisor of a and b.

A careful analysis (see e.g. Knuth [59, pp. 339ff]) shows that the Euclidean algorithm performs on the average $(12 \ln 2 \ln a)/\pi^2 \approx 1.9405 \log_{10} a$ steps (if $a > b > 0$) and at most $\log_\lambda a$ divisions, where $\lambda = (1 + \sqrt{5})/2$.

A direct consequence of Euclid's algorithm is the following important property of the greatest common divisor, showing that the greatest common divisor of a and b can always be expressed as a linear combination of a and b:

THEOREM 1.2 *Let a and b be integers with greatest common divisor d. Then, there exist integers x and y so that $d = ax + by$.*

Proof: We show by induction that every r_i (and thus also $r_n = d$) can be expressed as a linear combination of a and b. By setting $r_{-1} = a$ and $r_0 = b$, the claim is trivial for r_{-1} and r_0. Suppose now that every r_i with $i < k$ can be written as linear combination of a and b, i.e. there exist integers x_i and y_i with $r_i = x_i a + y_i b$. Then,

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= (x_{k-2}a + y_{k-2}b) - q_k(x_{k-1}a + y_{k-1}b) \\ &= a(x_{k-2} - q_k x_{k-1}) + b(y_{k-2} - q_k y_{k-1}) \end{aligned}$$

Setting $x_k = x_{k-2} - q_k x_{k-1}$ and $y_k = y_{k-2} - q_k y_{k-1}$ completes the proof. □

Note that the sequence x_i and y_i in the last proof is efficiently computable in a recursive manner. An extension of the Euclidean algorithm, which computes, besides the $d = \gcd(a, b)$ of two integers a and b, also the integers x and y of the last theorem, is called extended Euclidean algorithm and can be outlined as follows (the variables x and y represent the sequences x_i and y_i in the proof of Theorem 1.2):

if $b = 0$ **then** $d := a$; $x := 1$; $y := 0$; **exit end if**
$x_2 := 1$; $x_1 := 0$; $y_2 := 0$; $y_1 := 1$;
while $b > 0$
    $q := \lfloor a/b \rfloor$; $r := a - qb$; $x := x_2 - qx_1$; $y := y_2 - qy_1$;
    $a := b$; $b := r$; $x_2 := x_1$; $x_1 := x$; $y_2 := y_1$; $y_1 := y$;
end while
$d := a$; $x := x_2$; $y := y_2$;
return (d, x, y);

The least common multiple d of two integers a and b, written $\operatorname{lcm}(a, b)$ is a multiple of both a and b with the property that d divides every common multiple of a and b. Similar to the greatest common divisor, the least common multiple is unique up to multiplication with a unit; if we speak of the lcm in $\mathbb{Z}$, we always refer to the positive lcm. It is easy to show that $\operatorname{lcm}(a, b) = |ab| / \gcd(a, b)$.

An element p of any integral domain is called *prime*, if it is not a unit, not zero and the following condition holds: if p divides any product ab of elements of the integral domain, then p divides a or b. In special rings, called ZPE rings, primes are exactly those elements that are *irreducible*. An element p (which is neither a unit nor zero) is irreducible, if p equals a product ab then either a or b must be a unit. Such ZPE rings have the interesting property that any element can be uniquely written (up to arrangement of factors and multiplication with a unit) as product of primes.