

LYNN MARGARET BATTEN

PUBLIC KEY CRYPTOGRAPHY

Applications and Attacks

 **WILEY**

 **IEEE**
IEEE PRESS

IEEE Press Series on
Information & Communication
Networks Security
Stamatis Kartalopoulos, Series Editor

PUBLIC KEY CRYPTOGRAPHY



IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

IEEE Press Editorial Board 2012
John B. Anderson, *Editor in Chief*

Ramesh Abhari
George W. Arnold
Flavio Canavero
Dmitry Goldgof

Bernhard M. Haemmerli
David Jacobson
Mary Lanzerotti
Om P. Malik

Saeid Nahavandi
Tariq Samad
George Zobrist

Kenneth Moore, *Director of IEEE Book and Information Services (BIS)*

Technical Reviewer
Lejla Batina, *Radboud University Nijmegen, The Netherlands*

PUBLIC KEY CRYPTOGRAPHY

Applications and Attacks

Lynn Margaret Batten
Deakin University, Melbourne, Australia



IEEE Press

IEEE Press Series on
Information & Communication
• Networks Security
Stamatios Kartalopoulos, Series Editor



A John Wiley & Sons, Inc., Publication

Copyright © 2013 by The Institute of Electrical and Electronics Engineers, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Batten, Lynn Margaret.

Public key cryptography : applications and attacks / Lynn Margaret Batten.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-118-31712-9 (cloth)

1. Public key cryptography. 2. Cryptography--Mathematics. I. Title.
TK5102.94.B38 2012
005.8'2--dc23

2012025411

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For Glenn

“In the margin of his copy of Arithmetica, Pierre de Fermat had jotted the words ‘I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain . . .’ And all of a sudden she understood. The answer was disarmingly simple.”

(From ***The Girl Who Played with Fire*** by Stieg Larsson. Translated into English from the Swedish by Reg Keeland. Maclehorse Press, Quercus, London, 2009, p. 536)

CONTENTS

Preface	xiii
Acknowledgments	xv
List of Figures	xvii
1 INTRODUCTION	1
1.1 The Meaning of the Word Cryptography	2
1.2 Symmetric Key Cryptography	2
1.2.1 Impact of Technology	3
1.2.2 Confusion and Diffusion	3
1.2.3 DES and AES	4
1.3 Public Key (Asymmetric) Cryptography	5
1.3.1 Diffie–Hellman Key Exchange	5
1.3.2 RSA	5
1.3.3 ElGamal	6
1.4 Key Establishment	7
1.5 Cryptography—More than just Hiding Secrets	8
1.5.1 Digital Signatures	8
1.5.2 Authentication	9
1.5.3 Nonrepudiation	9
1.6 Standards	9
1.7 Attacks	10
2 CONGRUENCE EQUATIONS	13
2.1 Congruence Arithmetic	14
2.1.1 Computer Examples	17
2.1.2 Problems	18
2.2 The Euclidean Algorithm—Finding Inverses	18
2.2.1 Computer Examples	24
2.2.2 Problems	25
	vii

2.3	Discrete Logarithms and Diffie–Hellman Key Exchange	26
2.3.1	Computer Examples	32
2.3.2	Problems	33
2.4	Attacking the Discrete Logarithm	34
2.4.1	Computer Examples	41
2.4.2	Problems	42
3	THE ELGAMAL SCHEME	45
3.1	Primitive Roots	45
3.1.1	Computer Examples	50
3.1.2	Problems	51
3.2	The ElGamal Scheme	51
3.2.1	Computer Examples	53
3.2.2	Problems	55
3.3	Security of the ElGamal Scheme	56
3.3.1	Computer Examples	57
3.3.2	Problems	58
4	THE RSA SCHEME	59
4.1	Euler’s Theorem	59
4.1.1	Computer Examples	62
4.1.2	Problems	63
4.2	The RSA Algorithm	63
4.2.1	The RSA Parameters	66
4.2.2	Computer Examples	67
4.2.3	Problems	68
4.3	RSA Security	69
4.3.1	Computer Examples	74
4.3.2	Problems	76
4.4	Implementing RSA	76
4.4.1	Computer Examples	78
4.4.2	Problems	79
5	ELLIPTIC CURVE CRYPTOGRAPHY	81
5.1	Elliptic Curves and Elliptic Curve Groups	82
5.1.1	What is an Elliptic Curve?	82
5.1.2	Operations on Points	84

5.1.3	Adding a Point to Its Negative	86
5.1.4	Adding a Point to Itself	86
5.1.5	Computer Examples	90
5.1.6	Problems	91
5.2	Elliptic Curve Cryptography	92
5.2.1	Elliptic Curve Groups and the Discrete Logarithm Problem	92
5.2.2	An Elliptic Curve ElGamal System	93
5.2.3	Elliptic Curve Key Exchange (ECKE)	95
5.2.4	Computer Examples	96
5.2.5	Problems	98
5.3	The Elliptic Curve Factoring Scheme	99
5.3.1	Computer Examples	100
5.3.2	Problems	101
6	DIGITAL SIGNATURES	103
6.1	Hash Functions	104
6.1.1	SHA-1	108
6.1.2	MD5	109
6.1.3	The Search for New Hash Functions	112
6.1.4	Computer Examples	113
6.1.5	Problems	114
6.2	Digital Signature Schemes	116
6.2.1	Direct Digital Signature Schemes	116
6.2.2	Using RSA for Signing	117
6.2.3	Using ElGamal for Signing	118
6.2.4	Arbitrated Digital Signature Schemes	118
6.2.5	The Digital Signature Standard	119
6.2.6	Computer Examples	121
6.2.7	Problems	122
6.3	Attacks on Digital Signatures	123
6.3.1	The Birthday Attack	123
6.3.2	Intruder-in-the-Middle Attack	124
6.3.3	Intruder-in-the-Middle and Diffie–Hellman	125
6.3.4	An Attack on RSA Signatures: What if Eve Uses Alice’s Signature?	126
6.3.5	Protecting ElGamal with Signatures	127
6.3.6	Oscar Tries to Trick Bob	127
6.3.7	Oscar Captures a Message with a Signed Version	128

6.3.8	Alice Reuses a Random Number	129
6.3.9	Computer Examples	129
6.3.10	Problems	131
7	PRIMALITY TESTING	133
7.1	Fermat's Approach and Wilson's Theorem	134
7.1.1	Computer Examples	135
7.1.2	Problems	135
7.2	The Miller–Selfridge–Rabin Primality Test	136
7.2.1	The Miller–Selfridge–Rabin Algorithm (Long Version)	137
7.2.2	The MSR Algorithm (Short Version)	138
7.2.3	Computer Examples	140
7.2.4	Problems	140
7.3	True Primality Tests	141
7.3.1	Pocklington's Theorem	141
7.3.2	Proth's Theorem	142
7.3.3	Computer Examples	144
7.3.4	Problems	144
7.4	Mersenne Primes and the Lucas–Lehmer Test	144
7.4.1	The Lucas–Lehmer Test	145
7.4.2	Computer Examples	145
7.4.3	Problems	146
7.5	Primes is in P	146
7.5.1	Polynomial Rings	146
7.5.2	A Division Algorithm for Polynomials	147
7.5.3	A Euclidean Algorithm for Polynomials	147
7.5.4	Computer Examples	149
7.5.5	Problems	150
8	FACTORING METHODS	151
8.1	Fermat Again	152
8.1.1	Fermat's Difference of Squares Method	152
8.1.2	Using the Miller–Selfridge–Rabin Algorithm to Factor	153
8.1.3	Euler's Factoring Method	153
8.1.4	Kraitchik's Method	154
8.1.5	Computer Examples	155
8.1.6	Problems	156

8.2	The Quadratic Sieve	156
8.2.1	Computer Examples	158
8.2.2	Problems	159
8.3	Pollard's $p - 1$ and rho Methods	160
8.3.1	Pollard's $p - 1$ Method	160
8.3.2	The Pollard $p - 1$ Algorithm	160
8.3.3	Pollard's rho Method	161
8.3.4	The Pollard rho Algorithm	161
8.3.5	Computer Examples	162
8.3.6	Problems	163
8.4	Continued Fractions and Factoring	164
8.4.1	The Setup	164
8.4.2	Pell's Equation	167
8.4.3	Back to Factoring	167
8.4.4	Computer Examples	169
8.4.5	In Summary	171
8.4.6	Problems	171
	Appendix: Solutions to Problems	175
	Notation	193
	Bibliography	195
	Index	199

PREFACE

There are now many texts available giving an overview of both public key and symmetric key cryptography. The focus of this text is only the former. The objective is to give a complete description of the current major public key cryptosystems, the underlying mathematics, and the most common techniques used in attacking them.

It is assumed throughout that the reader has access to an algebraic software system such as Maple [65] or a sophisticated calculator supporting computation of large numbers and moduli. The reason for this is to emphasize the fact that, while the mathematical schemes are well designed, they supply no security unless they are implemented on sufficiently large values; thus, it is important to examine the complexity of the computations for small numbers as opposed to large ones. In each section of this book, we have provided computer-assisted examples.

The first chapters of this book cover the theory of public key systems in current use, including ElGamal, RSA, Elliptic Curve, and digital signature schemes. The underlying mathematics needed to build and study these schemes is provided as needed through the book. The latter half of the book examines attacks on these schemes via mathematical problems on which they are based fundamentally, the discrete logarithm problem and the difficulty of factoring integers.

The book is suitable for one or two semester courses for students with some discrete mathematics background including a knowledge of algorithms, computational complexity, and binary arithmetic. It is aimed at students studying cryptography in the context of information technology security and is designed to cover thoroughly the public key cryptography material needed for the writing of the CISSP exam [57]. It is equally aimed at mathematics students in the context of applications of groups and fields. Each chapter contains 40–50 problems and full solutions for the odd-numbered questions are provided in the appendix. To obtain the full solutions manual please send an email to: pressbooks@ieee.org.

LYNN MARGARET BATTEN

ACKNOWLEDGMENTS

I would like to thank Judy Chow for her considerable effort and skill in producing a LaTeX, version of this document. Bernard Colbert read and commented on several drafts, Martin Schulz assisted with Maple while Lei Pan produced elliptic curve graphics; I thank all of these people. In addition, I wish to thank Wiley representative Mary Hatcher and anonymous referees for their support and suggested improvements of the original manuscript.

LIST OF FIGURES

1.1	The M-209 encryption machine sold by Hagelin	4
1.2	Transmitting encrypted data over an insecure channel	7
1.3	Alice signs a message for Bob	8
2.1	A sequence cycle	35
4.1	The RSA challenge	65
5.1	An elliptic curve with real coefficients	83
5.2	Adding two distinct points	85
5.3	Adding a point to its negative	86
5.4	Doubling the point P	87
5.5	Doubling a point with tangent infinity	88
5.6	The graph of a finite elliptic curve	89
6.1	Cipher-block-chaining of an iterative hash function	107
6.2	The SHA-1 operations	108
6.3	The MD5 operations	110
6.4	Atul sends data to Antonio	111
6.5	Feena sends a document to Miriam	112
6.6	HashCalc	115
8.1	Factoring n	171

INTRODUCTION

This book is designed for use as a university text for year three, four, or honors level students. It is intended as a first approach to public key cryptography—no background in cryptography is needed. However, a basic understanding of discrete mathematics and algorithms and of the concept of computational complexity is assumed.

The major public key systems are presented in detail, both from the point of view of their design and their levels of security. Since all are based on a computationally difficult mathematical problem, the mathematics needed to construct and to analyze them is developed as needed along the way.

Each concept presented in the book comes with examples and problems, some of which can be done with limited computational capacity (a calculator for example) and some of which need major computational resources such as a mathematics-based software package or some independently written algorithms. Mathematica, Matlab, Magma [64], and Maple [65] are examples of packaged software that can be used easily to perform the necessary computations. For those who prefer open source software, see [28] where Sage is used for algorithms and examples. The book can be used without additional software resources by avoiding those problems which require them.

The software used by the author for the computationally expensive examples in this book was Maple. The solutions are presented with sufficient detail to permit an

easy translation to any other language or package. Full solutions are given to all odd-numbered problems. For those wishing to use the book at a Master's level, an emphasis on the computational complexity of the cryptographic systems and or the attacks on them would provide a solid basis for a good course including programme writing. *Emphasis on the computational complexity of attacks on public key systems provides the user with a feel for the level of security provided.*

1.1 THE MEANING OF THE WORD CRYPTOGRAPHY

In this preliminary chapter, we present some of the history of cryptography and the reasons for the development of the systems that we see in use today. There are no exercises associated with this chapter, but the interested reader can follow up any of the references and links provided.

The words “*cryptography*,” “*cryptology*,” and “*cryptanalysis*” are commonly interchanged. However, each of them has a slightly different meaning. The common beginning “crypt” comes from the Greek *κρυμμενοζ* or *kruptos* for “hidden.” The ending “graphy” refers to writing and so the first word in the list means “hidden writing” and generally refers to the encryption part of establishing a system for transmitting secrets. We call such an encrypted string a “cipher” or “ciphertext.” Normally, when a cipher is constructed, the idea is that there will be some person or persons who can “legitimately” decipher it and so find the hidden text. In order to legitimately decipher, it is understood that a person will hold what is referred to as a “key,” a means of simply and efficiently determining the original text. On the other hand, without this key, it should not be simple to deduce the hidden text.

The last word, cryptanalysis, refers to an analysis of hidden things, or ciphers, to expose what is hidden; this word generally refers to the decryption or discovery component of the system when the analyst does not have a legitimate key with which to read a cipher.

Finally, the word cryptology is made up of the two components “hidden” and “study” and refers to the study of hidden writings or secrets. This word encompasses both the establishment of encryption methods and the analysis of a cipher in order to break it without the associated key. While “cryptology” would be the correct word for a discussion including both encryption techniques and analysis of these techniques with the intent of breaking them, many people use the word “cryptography” instead.

In the next section, we cover very briefly the introduction of, and changes to, symmetric key cryptography over thousands of years. This is followed by a brief introduction to public key cryptography. Recent applications of cryptography, in addition to simply hiding data, are mentioned in Section 1.5. Section 1.6 mentions current standards in the area of cryptography and their impact.

1.2 SYMMETRIC KEY CRYPTOGRAPHY

The hiding of secrets in written and pictorial form with the intent of passing on a message to a select few has been documented over thousands of years, going far back in time to

ancient Egypt [2, 36]. In many cases, it was used as a game so that the select few were able to have access to information not available to those excluded from the inner circle. However, it was also used in times of political tension and war to communicate securely, guarding secret information from the enemy.

Symmetric key systems are cryptographic systems in which decrypting is a simple method of reversing the encryption used. For example, if a message written in English is encrypted by replacing each letter with the one five places ahead in the alphabet (*a* is replaced by *f*, *b* by *g*, and so on), then to decrypt, the letters are simply moved five places back. A message written as a binary string may be encrypted by adding it to another, fixed, binary string. To decrypt, adding the fixed binary string again will produce the original message. Thus, to use a symmetric key cryptographic scheme, both the sender and the receiver use essentially the same key.

The simplicity of using the same key both to encrypt and to decrypt is off set by the difficulty of ensuring that all parties have the needed keys in a tense situation, and also when people may be widely dispersed geographically. In time of war, keys have to be physically delivered to personnel even in the remotest and most dangerous locations. In the late 1800s, the idea of a “code book” which listed which keys to be used on which dates was born. Both the transmitter and the receiver needed a copy of the same code book for this to work, but several months of communications could be based on the delivery of a single code book. (Serious users of encryption recognized the need for constantly changing the key!)

1.2.1 Impact of Technology

Despite its history of about 4000 years, cryptography only came of age in the 1800s with the invention of technologies such as the telegraph (for rapid communication over great distances) and manual rotary machines, followed in the early 1900s by electrical rotary machines [2]. David Khan, in his book *The Code Breakers* [22] explains that the electro mechanical rotary machine for cryptographic purposes was invented almost simultaneously around 1917–1919 by four different people in four different countries. None of these people became rich. One of them, the Swede *Arvid Damm*, died in 1927 and his company was taken over by another Swede, *Boris Hagelin* (1892–1983). Despite Hagelin’s death, the company, Crypto AG (<http://www.crypto.ch/>), still operates in Zug, Switzerland. Figure 1.1 shows a machine sold by the company.

1.2.2 Confusion and Diffusion

As cryptography became less of an art form and more of a science in the 1900s, it was inevitable that at some point, someone would try to formalize the principal aims of a cryptographic system. Claude Shannon was one of the first to do so [48]. He argued that a cryptosystem designer should assume that the system may be attacked by someone who has access to it, as was indeed the case during the two world wars when machines were stolen and reverse engineered. He argued that the only point of secrecy should be the key, but that the system design should assist the security by incorporating “confusion” and “diffusion.” “Confusion is intended to make the relationship between the key and