LYNN MARGARET BATTEN

PUBLIC KEY CRYPTOGRAPHY

Applications and Attacks

WILEY

IEEE
IEEE PRESS

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

PUBLIC KEY CRYPTOGRAPHY

IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

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

PUBLIC KEY CRYPTOGRAPHY

Applications and Attacks

Lynn Margaret Batten
Deakin University, Melbourne, Australia

IEEE
IEEE Press

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

WILEY
A John Wiley & Sons, Inc., Publication

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

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. Maclehose Press, Quercus, London, 2009, p. 536)

CONTENTS

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

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

Public Key Cryptography: Applications and Attacks, First Edition. Lynn Margaret Batten.

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 "crytp" comes from the Greek $\kappa\rho\upsilon\mu\mu\epsilon\nu o\zeta$ 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