

Second Edition

Introduction to Cryptography with Coding Theory

Wade Trappe

*Wireless Information Network Laboratory
and the Electrical and Computer Engineering Department
Rutgers University*

Lawrence C. Washington

*Department of Mathematics
University of Maryland*




Pearson Education International

Introduction to Cryptography
with Coding Theory

If you purchase this book within the United States or Canada you should be aware that it has been wrongfully imported without the approval of the publisher or the Author.

Executive Acquisitions Editor: *George Lobell*
 Editor-in-Chief: *Sally Yagan*
 Production Editor: *Raegan Keida*
 Senior Managing Editor: *Linda Mihatov Behrens*
 Assistant Managing Editor: *Bayani Mendoza de Leon*
 Executive Managing Editor: *Kathleen Schiaparelli*
 Manufacturing Buyer: *Alan Fischer*
 Marketing Manager: *Halee Dinsey*
 Marketing Assistant: *JoonWon Moon*
 Cover Designer: *Bruce Kensehaar*
 Art Director: *Jayne Conte*
 Director of Creative Services: *Paul Belfanti*
 Manager, Cover Visual Research & Permissions: *Karen Sanatar*
 Editorial Assistant: *Jennifer Urban*
 Cover Image: *Pillowslip Square Dance by Collier Campbell Lifeworks. ©Collier Campbell Lifeworks/CORBIS*

 © 2006, 2002 Pearson Education, Inc.
 Pearson Prentice Hall
 Pearson Education, Inc.
 Upper Saddle River, NJ 07458

All rights reserved. No part of this book may be reproduced, in any form or by any means, without permission in writing from the publisher.

Pearson Prentice Hall™ is a trademark of Pearson Education, Inc.

"MATLAB" is a registered trademark and the L-shape of the membrane logo is a trademark of The Mathworks, Inc. used by permission.

Maple® is a registered trademark of MapleSoft, a division of Waterloo Maple, Inc.

Mathematica® is a registered trademark of Wolfram Research Inc.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN 0-13-198199-4

Pearson Education, Ltd., *London*
 Pearson Education Australia PTY. Limited, *Sydney*
 Pearson Education Singapore, Pte., Ltd
 Pearson Education North Asia Ltd, *Hong Kong*
 Pearson Education Canada, Ltd., *Toronto*
 Pearson Education de Mexico, S.A. de C.V.
 Pearson Education - Japan, *Tokyo*
 Pearson Education Malaysia, Pte. Ltd
 Pearson Education, Upper Saddle River, *New Jersey*

Contents

Preface	xi
1 Overview of Cryptography and Its Applications	1
1.1 Secure Communications	2
1.2 Cryptographic Applications	9
2 Classical Cryptosystems	12
2.1 Shift Ciphers	13
2.2 Affine Ciphers	14
2.3 The Vigenère Cipher	16
2.4 Substitution Ciphers	24
2.5 Sherlock Holmes	27
2.6 The Playfair and ADFGX Ciphers	30
2.7 Block Ciphers	34
2.8 Binary Numbers and ASCII	38
2.9 One-Time Pads	39
2.10 Pseudo-random Bit Generation	41
2.11 LFSR Sequences	43
2.12 Enigma	50
2.13 Exercises	55
2.14 Computer Problems	59
3 Basic Number Theory	63
3.1 Basic Notions	63
3.2 Solving $ax + by = d$	69
3.3 Congruences	70
3.4 The Chinese Remainder Theorem	76
3.5 Modular Exponentiation	78
3.6 Fermat and Euler	79
3.7 Primitive Roots	83
3.8 Inverting Matrices Mod n	85
3.9 Square Roots Mod n	86
3.10 Legendre and Jacobi Symbols	88
3.11 Finite Fields	93

3.12	Continued Fractions	102
3.13	Exercises	104
3.14	Computer Problems	111
4	The Data Encryption Standard	113
4.1	Introduction	113
4.2	A Simplified DES-Type Algorithm	114
4.3	Differential Cryptanalysis	118
4.4	DES	123
4.5	Modes of Operation	131
4.6	Breaking DES	139
4.7	Meet-in-the-Middle Attacks	143
4.8	Password Security	144
4.9	Exercises	146
4.10	Computer Problems	149
5	The Advanced Encryption Standard: Rijndael	151
5.1	The Basic Algorithm	152
5.2	The Layers	154
5.3	Decryption	158
5.4	Design Considerations	161
5.5	Exercises	162
6	The RSA Algorithm	164
6.1	The RSA Algorithm	164
6.2	Attacks on RSA	169
6.3	Primality Testing	176
6.4	Factoring	181
6.5	The RSA Challenge	187
6.6	An Application to Treaty Verification	189
6.7	The Public Key Concept	189
6.8	Exercises	192
6.9	Computer Problems	197
7	Discrete Logarithms	201
7.1	Discrete Logarithms	201
7.2	Computing Discrete Logs	202
7.3	Bit Commitment	209
7.4	Diffie-Hellman Key Exchange	210
7.5	The ElGamal Public Key Cryptosystem	212
7.6	Exercises	214
7.7	Computer Problems	216

8	Hash Functions	218
8.1	Hash Functions	218
8.2	A Simple Hash Example	222
8.3	The Secure Hash Algorithm	224
8.4	Birthday Attacks	229
8.5	Multicollisions	232
8.6	The Random Oracle Model	235
8.7	Using Hash Functions to Encrypt	238
8.8	Exercises	239
8.9	Computer Problems	242
9	Digital Signatures	244
9.1	RSA Signatures	245
9.2	The ElGamal Signature Scheme	246
9.3	Hashing and Signing	249
9.4	Birthday Attacks on Signatures	250
9.5	The Digital Signature Algorithm	251
9.6	Exercises	252
9.7	Computer Problems	255
10	Security Protocols	256
10.1	Intruders-in-the-Middle and Impostors	257
10.2	Key Distribution	259
10.3	Kerberos	266
10.4	Public Key Infrastructures (PKI)	270
10.5	X.509 Certificates	271
10.6	Pretty Good Privacy	277
10.7	SSL and TLS	280
10.8	Secure Electronic Transaction	283
10.9	Exercises	285
11	Digital Cash	287
11.1	Digital Cash	287
11.2	Exercises	294
12	Secret Sharing Schemes	296
12.1	Secret Splitting	296
12.2	Threshold Schemes	297
12.3	Exercises	303
12.4	Computer Problems	305

13 Games	307
13.1 Flipping Coins over the Telephone	307
13.2 Poker over the Telephone	309
13.3 Exercises	314
14 Zero-Knowledge Techniques	316
14.1 The Basic Setup	316
14.2 The Feige-Fiat-Shamir Identification Scheme	319
14.3 Exercises	321
15 Information Theory	325
15.1 Probability Review	326
15.2 Entropy	328
15.3 Huffman Codes	333
15.4 Perfect Secrecy	335
15.5 The Entropy of English	338
15.6 Exercises	343
16 Elliptic Curves	347
16.1 The Addition Law	347
16.2 Elliptic Curves Mod p	352
16.3 Factoring with Elliptic Curves	356
16.4 Elliptic Curves in Characteristic 2	360
16.5 Elliptic Curve Cryptosystems	363
16.6 Identity-Based Encryption	366
16.7 Exercises	370
16.8 Computer Problems	374
17 Lattice Methods	376
17.1 Lattices	376
17.2 Lattice Reduction	377
17.3 An Attack on RSA	382
17.4 NTRU	385
17.5 Exercises	390
18 Error Correcting Codes	392
18.1 Introduction	392
18.2 Error Correcting Codes	398
18.3 Bounds on General Codes	402
18.4 Linear Codes	408
18.5 Hamming Codes	416
18.6 Golay Codes	417
18.7 Cyclic Codes	426
18.8 BCH Codes	432

18.9 Reed-Solomon Codes	440
18.10 The McEliece Cryptosystem	442
18.11 Other Topics	444
18.12 Exercises	445
18.13 Computer Problems	449
19 Quantum Techniques in Cryptography	450
19.1 A Quantum Experiment	451
19.2 Quantum Key Distribution	454
19.3 Shor's Algorithm	456
19.4 Exercises	466
A Mathematica® Examples	467
A.1 Getting Started with Mathematica	467
A.2 Some Commands	469
A.3 Examples for Chapter 2	470
A.4 Examples for Chapter 3	477
A.5 Examples for Chapter 6	480
A.6 Examples for Chapter 8	487
A.7 Examples for Chapter 12	487
A.8 Examples for Chapter 13	488
A.9 Examples for Chapter 16	490
B Maple® Examples	495
B.1 Getting Started with Maple	495
B.2 Some Commands	496
B.3 Examples for Chapter 2	498
B.4 Examples for Chapter 3	505
B.5 Examples for Chapter 6	509
B.6 Examples for Chapter 8	517
B.7 Examples for Chapter 12	518
B.8 Examples for Chapter 13	519
B.9 Examples for Chapter 16	521
C MATLAB® Examples	527
C.1 Getting Started with MATLAB	528
C.2 Examples for Chapter 2	533
C.3 Examples for Chapter 3	544
C.4 Examples for Chapter 6	548
C.5 Examples for Chapter 8	553
C.6 Examples for Chapter 12	553
C.7 Examples for Chapter 13	554
C.8 Examples for Chapter 16	556

D Suggestions for Further Reading	564
Bibliography	565
Index	571

Preface

This book is based on a course in cryptography at the upper-level undergraduate and beginning graduate level that has been given at the University of Maryland since 1997, and a course that has been taught at Rutgers University since 2003. When designing the courses, we decided on the following requirements:

- The courses should be up-to-date and cover a broad selection of topics from a mathematical point of view.
- The material should be accessible to mathematically mature students having little background in number theory and computer programming.
- There should be examples involving numbers large enough to demonstrate how the algorithms really work.

We wanted to avoid concentrating solely on RSA and discrete logarithms, which would have made the courses mostly about number theory. We also did not want to focus on protocols and how to hack into friends' computers. That would have made the courses less mathematical than desired.

There are numerous topics in cryptology that can be discussed in an introductory course. We have tried to include many of them. The chapters represent, for the most part, topics that were covered during the different semesters we taught the course. There is certainly more material here than could be treated in most one-semester courses. The first nine chapters represent the core of the material. The choice of which of the remaining chapters are used depends on the level of the students and the objectives of the lecturer.

The chapters are numbered, thus giving them an ordering. However, except for Chapter 3 on number theory, which pervades the subject, the chapters are fairly independent of each other and can be covered in almost any

reasonable order. Although we don't recommend doing so, a daring reader could possibly read Chapters 4 through 19 in reverse order, with only having to look ahead/behind a few times. Since students have varied backgrounds in number theory, we have collected the basic number theory facts together in Chapter 3 for ease of reference; however, we recommend introducing these concepts gradually throughout the course as they are needed.

The chapters on information theory, elliptic curves, quantum cryptography, lattice methods, and error correcting codes are somewhat more mathematical than the others. The chapter on error correcting codes was included, at the suggestion of several reviewers, because courses that include introductions to both cryptology and coding theory are fairly common.

Computer examples. Suppose you want to give an example for RSA. You could choose two one-digit primes and pretend to be working with fifty-digit primes, or you could use your favorite software package to do an actual example with large primes. Or perhaps you are working with shift ciphers and are trying to decrypt a message by trying all 26 shifts of the ciphertext. This should also be done on a computer. At the end of the book are appendices containing computer examples written in each of Mathematica®, Maple®, and MATLAB® that show how to do such calculations. These languages were chosen because they are user friendly and do not require prior programming experience. Although the course has been taught successfully without computers, these examples are an integral part of the book and should be studied, if at all possible. Not only do they contain numerical examples of how to do certain computations but also they demonstrate important ideas and issues that arise. They were placed at the end of the book because of the logistic and aesthetic problems of including extensive computer examples in three languages at the ends of chapters.

Programs available in each of the three languages can be downloaded from the Web site

www.prenhall.com/washington

In a classroom, all that is needed is a computer (with one of the languages installed) and a projector in order to produce meaningful examples as the lecture is being given. Homework problems (the computer problems in various chapters) based on the software allow students to play with examples individually. Of course, students having more programming background could write their own programs instead.

What is new in the second edition. Cryptography is a quickly changing field. Since the first edition of this book appeared, there have been significant developments regarding hash functions and identity-based encryption, for example. These necessitated updates to the material. Many

people also made suggestions for the exposition, and there were several requests for more exercises. The main additions we made are as follows:

1. Many new exercises, especially in Chapters 2, 3, 5, 6, and 16.
2. New and expanded material on hash functions, collected into a new chapter (Chapter 8).
3. A new chapter (Chapter 10) on security protocols.
4. A new chapter (Chapter 17) on lattice methods.
5. A section on identity-based encryption in Chapter 16.
6. New sections on Legendre and Jacobi symbols and on continued fractions in Chapter 3.
7. More modes of operation in Chapter 4.
8. More attacks on RSA in Chapter 6.

We of course welcome suggestions and corrections. An errata page can be found at the website for the book: *www.prenhall.com/washington*. A solutions manual, *for instructors only*, can be obtained from the mathematics editors or publisher's representatives of Prentice Hall.

Acknowledgments. Many people helped and provided encouragement during the preparation of this book. First, we would like to thank our students, whose enthusiasm, insights, and suggestions contributed greatly. We are especially grateful to many people who have provided corrections and other input, especially our colleagues Bill Gasarch and Jeff Adams. Jonathan Rosenberg and Tim Strobell provided invaluable technical assistance. We would like to thank Wenyuan Xu, Qing Li, and Pandurang Kamat, who drew several of the diagrams and provided feedback on the new material for the second edition. The reviewers deserve special thanks: for the first edition: David Grant (University of Colorado at Boulder), David M. Pozar (University of Massachusetts, Amherst), Jugal K. Kalita (University of Colorado at Colorado Springs), Anthony Ephremides (University of Maryland, College Park), J. Felipe Voloch (University of Texas at Austin), Agnes Chan (Northeastern University), Daniel F. Warren (Naval Postgraduate School), and one anonymous reviewer; and for the second edition: Eric Bach (University of Wisconsin), James W. Brewer (Florida Atlantic University), Siman Wong (University of Massachusetts, Amherst), Thomas P. Cahill (Brooklyn Polytechnic University), and Edmund Lamagna (University of Rhode Island). Their suggestions on the exposition and the organization of the topics greatly enhanced the final result. We have enjoyed working with

the staff at Prentice Hall, especially the mathematics editor, George Lobell, and the production editors Jeanne Audino (first edition) and Raegan Keida (second edition).

The first author would like to thank Nisha Gilra, who provided encouragement and advice; Sheilagh O'Hare for introducing him to the field of cryptography; and K.J. Ray Liu for his support.

The second author thanks Susan Zengerle and Patrick Washington for their patience, help, and encouragement during the writing of this book.

Wade Trappe
trappe@winlab.rutgers.edu

Lawrence C. Washington
lcw@math.umd.edu