*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

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 Kenselaar*
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*



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



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

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*