# 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 thirteen 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. 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.

Additionally, at the end of the book are appendices containing computer examples written in each of Mathematica®, Maple®, MATLAB®, and Sage 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 these languages at the ends of chapters.

Additionally, programs available in Mathematica, Maple, and MATLAB can be downloaded from the Web site (`bit.ly/2JbcS6p`). 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. 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.

**New to the Third Edition.** Two major changes have informed this edition: Changes to the field of cryptography and a change in the format of the text. We address these issues separately, although there is an interplay between the two:

**Content Changes.** Cryptography is a quickly changing field. We have made many changes to the text since the last edition:

- Reorganized content previously in two chapters to four separate chapters on Stream Ciphers (including RC4), Block Ciphers, DES and AES (Chapters 5–8, respectively). The RC4 material, in particular, is new.

- Heavily revised the chapters on hash functions. Chapter 11 (Hash functions) now includes sections on SHA-2 and SHA-3. Chapter 12 (Hash functions: Attacks and Applications) now includes material on message authentication codes, password protocols, and blockchains.

- The short section on the one-time pad has been expanded to become Chapter 4, which includes sections on multiple use of the one-time pad, perfect secrecy, and ciphertext indistinguishability.

- Added Chapter 14, "What Can Go Wrong," which shows what can happen when cryptographic algorithms are used or designed incorrectly.

- Expanded Chapter 16 on digital cash to include Bitcoin and cryptocurrencies.
- Added Chapter 22, which gives an introduction to Pairing-Based Cryptography.
- Updated the exposition throughout the book to reflect recent developments.
- Added references to the Maple, Mathematica, MATLAB, and Sage appendices in relevant locations in the text.
- Added many new exercises.
- Added a section at the back of the book that contains answers or hints to a majority of the odd-numbered problems.

**Format Changes.** A focus of this revision was transforming the text from a print-based learning tool to a digital learning tool. The eText is therefore filled with content and tools that will help bring the content of the course to life for students in new ways and help improve instruction. Specifically, the following are features that are available only in the eText:

- Interactive Examples. We have added a number of opportunities for students to interact with content in a dynamic manner in order to build or enhance understanding. Interactive examples allow students to explore concepts in ways that are not possible without technology.
- Quick Questions. These questions, built into the narrative, provide opportunities for students to check and clarify understanding. Some help address potential misconceptions.
- Notes, Labels, and Highlights. Notes can be added to the eText by instructors. These notes are visible to all students in the course, allowing instructors to add their personal observations or directions to important topics, call out need-to-know information, or clarify difficult concepts. Students can add their own notes, labels, and highlights to the eText, helping them focus on what they need to study. The customizable Notebook allows students to filter, arrange, and group their notes in a way that makes sense to them.
- Dashboard. Instructors can create reading assignments and see the time spent in the eText so that they can plan more effective instruction.
- Portability. Portable access lets students read their eText whenever they have a moment in their day, on Android and iOS mobile phones and tablets. Even without an Internet connection, offline reading ensures students never miss a chance to learn.
- Ease-of-Use. Straightforward setup makes it easy for instructors to get their class up and reading quickly on the first day of class. In addition, Learning Management System (LMS) integration provides institutions, instructors, and students with single sign-on access to the eText via many popular LMSs.

- Supplements. An Instructors' Solutions Manual can be downloaded by qualified instructors from the textbook's webpage at `www.pearson.com`.

**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 Bill Gasarch, Jeff Adams, Jonathan Rosenberg, and Tim Strobell. 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. We have enjoyed working with the staff at Pearson, especially Jeff Weidenaar and Tara Corpuz.

The reviewers deserve special thanks: their suggestions on the exposition and the organization of the topics greatly enhanced the final result. The reviewers marked with an asterisk (*) provided input for this edition.

* Anurag Agarwal, Rochester Institute of Technology
* Pradeep Atrey, University at Albany
  Eric Bach, University of Wisconsin
  James W. Brewer, Florida Atlantic University
  Thomas P. Cahill, NYU
  Agnes Chan, Northeastern University
* Nathan Chenette, Rose-Hulman Institute of Technology
* Claude Crépeau, McGill University
* Reza Curtmola, New Jersey Institute of Technology
* Ahmed Desoky, University of Louisville
  Anthony Ephremides, University of Maryland, College Park
* David J. Fawcett, Lawrence Tech University
* Jason Gibson, Eastern Kentucky University
* K. Gopalakrishnan, East Carolina University
  David Grant, University of Colorado, Boulder
  Jugal K. Kalita, University of Colorado, Colorado Springs
* Saroja Kanchi, Kettering University
* Andrew Klapper, University of Kentucky
* Amanda Knecht, Villanova University
  Edmund Lamagna, University of Rhode Island
* Aihua Li, Montclair State University
* Spyros S. Magliveras, Florida Atlantic University
* Nathan McNew, Towson University
* Nick Novotny, IUPUI
  David M. Pozar, University of Massachusetts, Amherst
* Emma Previato, Boston University
* Hamzeh Roumani, York University
* Bonnie Saunders, University of Illinois, Chicago
* Ravi Shankar, University of Oklahoma
* Ernie Stitzinger, North Carolina State
* Armin Straub, University of South Alabama
  J. Felipe Voloch, University of Texas, Austin
  Daniel F. Warren, Naval Postgraduate School
* Simon Whitehouse, Alfred State College

Siman Wong, University of Massachusetts, Amherst
* Huapeng Wu, University of Windsor

Wade thanks 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. Larry thanks Susan Zengerle and Patrick Washington for their patience, help, and encouragement during the writing of this book.

Of course, we welcome suggestions and corrections. An errata page can be found at (`bit.ly/2J8nN0w`) or at the link on the book's general Web site (`bit.ly/2T544yu`).

Wade Trappe *trappe@winlab.rutgers.edu*

Lawrence C. Washington *lcw@math.umd.edu*