Cryptography and Secure Communication

Today's pervasive computing and communications networks have created an intense need for secure and reliable cryptographic systems. Bringing together a fascinating mixture of topics in engineering, mathematics, computer science, and informatics, this book presents the timeless mathematical theory underpinning cryptosystems both old and new.

Major branches of classical and modern cryptography are discussed in detail, from basic block and stream cyphers through to systems based on elliptic and hyperelliptic curves, accompanied by concise summaries of the necessary mathematical background. Practical aspects such as implementation, authentication, and protocol-sharing are also covered, as are the possible pitfalls surrounding cryptographic methods.

Written specifically with engineers in mind, and providing a solid grounding in the relevant algorithms, protocols, and techniques, this insightful introduction to the foundations of modern cryptography is ideal for graduate students and researchers in engineering and computer science, and practitioners involved in the design of security systems for communications networks.

Richard E. Blahut is the Henry Magnuski Professor of Electrical and Computer Engineering at the University of Illinois, Urbana–Champaign. He is a Fellow of the Institute of Electrical and Electronics Engineers and the recipient of many awards including the IEEE Alexander Graham Bell Medal (1998), the IEEE Claude E. Shannon Award, the Tau Beta Pi Daniel C. Drucker Eminent Faculty Award, and the IEEE Millennium Medal. He was named a Fellow of IBM Corporation in 1980 (where he worked for over 30 years) and was elected to the US National Academy of Engineering in 1990.

Cryptography and Secure Communication

Richard E. Blahut

Henry Magnuski Professor of Electrical and Computer Engineering,
University of Illinois, Urbana–Champaign

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Published in the United States of America by Cambridge University Press, New York

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107014275

First published 2014

Printed in the United Kingdom by TJ International Ltd. Padstow Cornwall

A catalog record for this publication is available from the British Library

ISBN 978-1-107-01427-5 Hardback

Yet it may be roundly asserted that human
ingenuity cannot concoct a cipher which
human ingenuity cannot resolve.

– Edgar Allen Poe
The Gold Bug

A hundred ounces of silver spent for information
may save ten thousand spent on war.

– Sun-Tzu
4th century AD

Cambridge University Press
978-1-107-01427-5 - Cryptography and Secure Communication
Richard E. Blahut
Frontmatter
More information

Contents

Preface

Information transmission and information protection are two sides of the same tapestry, but with the information-protection side having more tangled and multitextured threads. At the core of the subject of information protection is the more specific subject of classical cryptography, which protects the content of a message from being understood by unauthorized receivers, but does not protect the message in other ways. Much of this book is concerned with cryptography in this classical sense, but treated in its modern sophisticated form. The modern subject of cryptography, and of information protection in general, is a fascinating mixture of mathematics, engineering, informatics, and computer science, and the same mixture is found in this book.

The subject of information protection is rapidly evolving into a subject that goes well beyond the classical notions of point-to-point cryptography. Now there is an intense need for secrecy and security in large public networks. Within this larger setting of public networked communication, many other issues are important, including issues of authorization, certification, and authentication, that bring many subtle considerations into the discussion. While the emphasis of the book is cryptography, it touches on these other topics as well. My goal, as in my other books, is to concentrate on the formal, and presumably timeless, aspects of the subject rather than on the details of systems in current use. Although this book is not designed to serve as a handbook describing the current standard cryptosystems, some topics are best described by discussing practical systems that are now in use.

Modern cryptography uses a great deal of rather advanced mathematical material from the subjects of number theory, abstract algebra, and algebraic geometry, and I believe that one cannot be an expert in the subject of cryptography without having some understanding of this material. Accordingly, this book provides a formal and rigorous development of all relevant mathematical topics, but abridged to suit the needs of the moment.

This book was written by an engineer, a noncryptographer, for those – especially engineers – who want to learn the subject of information protection in some depth. While I readily admit to the dangers of this recipe, I also hope that there will be positive pedagogical consequences. As an outsider to the subject, I can more easily see when points that are obvious to the expert can be opaque to the novice, and so require more careful treatment. But, at the same time, I also believe strongly that the engineering student of cryptography must not be shortchanged. Though the starting background may be different than that of a mathematician, the engineer can and should follow the main flow of the mathematics to the core, not taking any of the fundamentals for granted.

In writing this book, I sometimes had to find my own way to a result that is beyond my formal training. For this reason, the development is goal-focused and direct, but without sacrificing rigor. My hope is that such a book written by a nonspecialist in a specialized subject will be accessible to the general technically educated reader.

Of course, the soft underbelly of much of modern cryptography is the subject of complexity, a subject that is not formally addressed in this book. Secrets are protected by the apparent intractability of the computational problem that is presented to the adversary. Evidence for intractability is often anecdotal. Formal statements, when known, are qualified, and often may apply only obliquely. Statements regarding the complexity usually refer to the asymptotic complexity, which is of theoretical interest, but can be very different from the practical complexity of real instances of the problem. Because our preference is to try to avoid unsupported assertions in this book, many statements regarding complexity often appear only in general terms, or in the end-of-chapter notes.

Most major notions of classical and modern cryptography are discussed in this book. Even some techniques that are out of date or discredited are discussed if they are important to the history and culture of the subject. Such ideas contribute to understanding, and may lead to future developments.

Many of the various topics of mathematics that underlie the subject of cryptography are gathered midway through the book, not appearing until Chapter 9, although the relevant elements of number theory do appear earlier in Chapter 2. The deferred placement of background material in Chapter 9 helps to shape the character of the book, but it necessitates the occasional forward-reference to the definitions and theorems of Chapter 9. The first half of the book – Chapters 1 through 8 – discusses classical cryptography and the basic earlier methods of public-key cryptography, mostly those based on number theory. The mathematics required in this half of the book is primarily number theory, which is developed in Chapter 2, and elementary notions of group theory. Public-key cryptography is studied in Chapters 3 and 4. Information-theoretic issues are studied in Chapter 5, conventional block and stream ciphers are studied in Chapters 6 and 7, and message authentication is covered in Chapter 8.

At the midpoint of the book, in Chapter 9, a concise summary is given of the mathematics that is needed throughout the latter chapters and occasionally in the early chapters. The latter half of the book also requires other advanced topics of mathematics, especially notions of algebraic geometry. For the most part, these topics are developed in place, as needed. In particular, cryptography based on elliptic and hyperelliptic curves, including pairing methods, is presented in Chapters 10, 11, and 12. The last three chapters round out the book. Chapter 13 discusses practical issues of implementation. Chapter 14 discusses identification, and Chapter 15 discusses lattice-based and code-based cryptography. Most of the treatment throughout is self-contained, or so it is intended.

The mathematics that is developed, beautiful and elegant, is in some ways related to the engineering mathematics of signal processing, though far more advanced and expressed in its own language. Perhaps some of this theory will one day pass into the engineer's workaday toolbox.

Acknowledgments

This book began as an assortment of unedited lecture notes from a course on cryptography that I taught in 1999 with Professor Nigel Boston, and repeated in 2003 and 2005 with Professor Iwan Duursma. Those early lecture notes were only intended to clarify the lectures as an aid to the class participants, and to help me with my own understanding of the mathematical material. Because of the many rough edges at that time, those notes were not intended for general distribution. The notes continued to evolve into the current book from 2009 to 2011 when I taught the course alone to mostly engineering students.

I owe my understanding of the deeper mathematical topics to my shared time with Boston both in the classroom and out of the classroom, as well as my interactions with Duursma. Without the closeness of this association, I could not have developed my understanding of this material. Although I do thank them for giving me this new interest, I also blame them for burdening me with a new addiction. My long friendships with Ian Blake and Jim Massey must also be mentioned as two early feathers tickling the skin of my curiosity. This book resulted from scratching that itch. And, of course, the stimulation and challenge of the many attentive and questioning students in the ECE Illinois classroom is invaluable in preparing a book such as this.

Expert criticism of the manuscript was kindly provided by Professor Nigel Boston, Professor Alfred Menezes, and Professor Ian F. Blake. Their help was invaluable and saved me from many errors. Early conversations with Negar Kiyavash, Sam Spencer, Patricio Parada, Figen Oktem, Sara Bahramian, and Leila Fuladi also helped me with the evolution of the manuscript. The quality of the book has much to do with the composition skills of Ms. Frances Bridges who provided that and so much more, and with the editing skills of Ms. Debra Rosenblum. And, as always, Barbara made it possible.

