CAMBRIDGE

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

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.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

Cryptography and Secure Communication

Richard E. Blahut

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

CAMBRIDGE
UNIVERSITY PRESS

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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

© Cambridge University Press 2014

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

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

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

Contents

Preface *page* xv
Acknowledgments xix

1 Introduction 1

1.1 Classical cryptography 2
1.2 Notions of cryptographic secrecy 5
1.3 Block ciphers 7
1.4 Stream ciphers 11
1.5 Public-key cryptography 13
1.6 Iterated and cascade ciphers 14
1.7 Cryptanalysis 15
1.8 Implementation attacks 18
1.9 Complexity theory 19
1.10 Authentication and identification 21
1.11 Ownership protection 23
1.12 Covert communications 24
1.13 History of information protection 25

2 The integers 32

2.1 Basic number theory 32
2.2 The euclidean algorithm 38
2.3 Prime fields 41
2.4 Quadratic residues 42
2.5 Quadratic reciprocity 47
2.6 The Jacobi symbol 51
2.7 Primality testing 55

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

2.8 The Fermat algorithm 56
2.9 The Solovay–Strassen algorithm 59
2.10 The Miller–Rabin algorithm 61
2.11 Factoring of integers 65
2.12 The Pollard algorithm for factoring 67
2.13 Square roots in a prime field 69

3 Cryptography based on the integer ring 82

3.1 Biprime cryptography 83
3.2 Implementing biprime cryptography 85
3.3 Protocol attacks on biprime cryptography 87
3.4 Direct attacks on biprime encryption 89
3.5 Factoring biprimes 90
3.6 The quadratic sieve 91
3.7 The number-field sieve 95
3.8 The Rabin cryptosystem 99
3.9 The rise and fall of knapsack cryptosystems 102

4 Cryptography based on the discrete logarithm 107

4.1 Diffie–Hellman key exchange 107
4.2 Discrete logarithms 109
4.3 The Elgamal cryptosystem 110
4.4 Trapdoor one-way functions 112
4.5 The Massey–Omura cryptosystem 113
4.6 The Pohlig–Hellman algorithm 114
4.7 The Shanks algorithm 121
4.8 The Pollard algorithm for discrete logarithms 123
4.9 The method of index calculus 127
4.10 Complexity of the discrete-log problem 129

5 Information-theoretic methods in cryptography 135

5.1 Probability space 136
5.2 Entropy 137
5.3 Perfect secrecy 139

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

5.4 The Shannon–McMillan theorem 141
5.5 Unicity distance 144
5.6 Entropy of natural language 147
5.7 Entropy expansion 149
5.8 Data compaction 150
5.9 The wiretap channel 152

6 Block ciphers 160

6.1 Block substitution 160
6.2 The Feistel network 162
6.3 The Data Encryption Standard 164
6.4 Using the Data Encryption Standard 168
6.5 Double and triple DES encryption 170
6.6 The Advanced Encryption Standard 171
6.7 Differential cryptanalysis 176
6.8 Linear cryptanalysis 177

7 Stream ciphers 181

7.1 State-dependent encryption 182
7.2 Additive stream ciphers 183
7.3 Linear shift-register sequences 185
7.4 The linear-complexity attack 189
7.5 Analysis of linear complexity 190
7.6 Keystreams from nonlinear feedback 194
7.7 Keystreams from nonlinear combining 196
7.8 Keystreams from nonlinear functions 199
7.9 The correlation attack 207
7.10 Pseudorandom sequences 210
7.11 Nonlinear sets of sequences 212

8 Authentication and ownership protection 218

8.1 Authentication 219
8.2 Identification 219
8.3 Authentication signatures 220

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

8.4 Hash functions 223
8.5 The birthday attack 225
8.6 Iterated hash constructions 227
8.7 Formal hash functions 228
8.8 Practical hash functions 230

9 Groups, rings, and fields 238

9.1 Groups 239
9.2 Rings 242
9.3 Fields 243
9.4 Prime fields 245
9.5 Binary fields and ternary fields 246
9.6 Univariate polynomials 247
9.7 Extension fields 255
9.8 The multiplication cycle in a finite field 261
9.9 Cyclotomic polynomials 263
9.10 Vector spaces 267
9.11 Linear algebra 269
9.12 The Fourier transform 272
9.13 Existence of finite fields 276
9.14 Bivariate polynomials 281
9.15 Modular reduction and quotient groups 285
9.16 Factoring of univariate polynomials 287

10 Cryptography based on elliptic curves 294

10.1 Elliptic curves 295
10.2 Elliptic curves over finite fields 300
10.3 The operation of point addition 303
10.4 The order of an elliptic curve 308
10.5 The group of an elliptic curve 310
10.6 Supersingular elliptic curves 312
10.7 Elliptic curves over binary fields 315
10.8 Computation of point multiples 319
10.9 Elliptic curve cryptography 320
10.10 The projective plane 323
10.11 Point counting in an extension field 325

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

10.12 Morphisms of elliptic curves over the rationals 333
10.13 Morphisms of elliptic curves over finite fields 337
10.14 Point counting in a ground field 343
10.15 The method of xedni calculus 347
10.16 Elliptic curves and the complex field 351
10.17 Curves constructed using complex multiplication 355

11 Cryptography based on hyperelliptic curves 369

11.1 Hyperelliptic curves 369
11.2 Coordinate rings and function fields 374
11.3 Poles and zeros 376
11.4 Divisors 379
11.5 Principal divisors 383
11.6 Principal divisors on elliptic curves 385
11.7 Jacobians as quotient groups 390
11.8 The group of a hyperelliptic curve 392
11.9 Semireduced divisors and jacobians 394
11.10 The Mumford transform 396
11.11 The Cantor reduction algorithm 402
11.12 Reduced divisors and jacobians 405
11.13 The Cantor–Koblitz algorithm 406
11.14 Hyperelliptic-curve cryptography 411
11.15 Order of the hyperelliptic jacobians 412
11.16 Some examples of the jacobian group 414

12 Cryptography based on bilinear pairings 422

12.1 Bilinear pairings 423
12.2 Pairing-based cryptography 425
12.3 Pairing-based key exchange 426
12.4 Identity-based encryption 428
12.5 Pairing-based signatures 431
12.6 Attacks on the bilinear Diffie–Hellman protocol 432
12.7 Torsion points and embedding degree 433
12.8 The torsion structure theorem 438
12.9 The structure of a pairing 446
12.10 Attacks using bilinear pairings 448

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

12.11 The Tate pairing 451
12.12 The Miller algorithm 457
12.13 The Weil pairing 460
12.14 Pairing-friendly curves 464
12.15 Barreto–Naehrig elliptic curves 465
12.16 More pairing-friendly curves 468

13 Implementation 475

13.1 Pairing enhancements 476
13.2 Accelerated pairings 478
13.3 Doubling and tripling 482
13.4 Point representations 484
13.5 Algorithms for elliptic-curve arithmetic 486
13.6 Modular addition in an integer ring 487
13.7 Modular multiplication in an integer ring 488
13.8 Representations of binary fields 491
13.9 Multiplication and squaring in a binary field 495
13.10 Complementary bases 500
13.11 Division in a finite field 503

14 Cryptographic protocols for security and identification 508

14.1 Protocols for cryptographic security 509
14.2 Identification protocols 510
14.3 Zero-knowledge protocols 512
14.4 Methods of secure identification 513
14.5 Signature protocols 519
14.6 Protocols for secret sharing 524

15 More public-key cryptography 527

15.1 Introduction to lattices 528
15.2 Elementary problems in lattice theory 535
15.3 Reduction of a lattice basis 536
15.4 Lattice-based cryptography 543
15.5 Attacks on lattice cryptosystems 547

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

15.6 Introduction to codes 548
15.7 Subspace projection 552
15.8 Code-based cryptography 553

Bibliography 558
Index 576

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

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

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.

© in this web service Cambridge University Press www.cambridge.org