DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

INTRODUCTION TO CRYPTOGRAPHY WITH OPEN-SOURCE SOFTWARE

Alasdair McAndrew

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

INTRODUCTION TO CRYPTOGRAPHY WITH OPEN-SOURCE SOFTWARE

Alasdair McAndrew

Victoria University
Melbourne, Victoria, Australia

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an Informa business
A CHAPMAN & HALL BOOK

Contents

Preface xv

1 Introduction to cryptography 1
- 1.1 Hiding information: Confidentiality 1
- 1.2 Some basic definitions 3
- 1.3 Attacks on a cryptosystem 5
- 1.4 Some cryptographic problems 7
- 1.5 Cryptographic protocols 8
- 1.6 Some simple ciphers 12
- 1.7 Cryptography and computer security 18
- 1.8 Glossary 19
- Exercises 20

2 Basic number theory 23
- 2.1 Introduction 23
- 2.2 Some basic definitions 23
- 2.3 Some number theoretic calculations 27
- 2.4 Primality testing 44
- 2.5 Glossary 47
- Exercises 48

3 Classical cryptosystems 55
- 3.1 Introduction 55
- 3.2 The Caesar cipher 56
- 3.3 Translation ciphers 57
- 3.4 Transposition ciphers 58
- 3.5 The Vigenère cipher 61
- 3.6 The one-time pad 65
- 3.7 Permutation ciphers 65
- 3.8 Matrix ciphers 66
- 3.9 Glossary 71
- Exercises 71

4 Introduction to information theory 79
- 4.1 Entropy and uncertainty 79

4.2 Perfect secrecy 82
4.3 Estimating the entropy of English 84
4.4 Unicity distance 88
4.5 Glossary 89
Exercises 89

5 Public-key cryptosystems based on factoring **93**
5.1 Introduction 93
5.2 The RSA cryptosystem 93
5.3 Attacks against RSA 99
5.4 RSA in Sage 101
5.5 Rabin's cryptosystem 104
5.6 Rabin's cryptosystem in Sage 109
5.7 Some notes on security 111
5.8 Factoring 112
5.9 Glossary 115
Exercises 115

6 Public-key cryptosystems based on logarithms and knapsacks **119**
6.1 El Gamal's cryptosystem 119
6.2 El Gamal in Sage 122
6.3 Computing discrete logarithms 125
6.4 Diffie–Hellman key exchange 127
6.5 Knapsack cryptosystems 128
6.6 Breaking the knapsack 137
6.7 Glossary 139
Exercises 140

7 Digital signatures **145**
7.1 Introduction 145
7.2 RSA signature scheme 147
7.3 Rabin digital signatures 150
7.4 The El Gamal digital signature scheme 152
7.5 The Digital Signature Standard 157
7.6 Glossary 161
Exercises 162

8 Block ciphers and the data encryption standard **167**
8.1 Block ciphers 167
8.2 Some definitions 169
8.3 Substitution/permutation ciphers 171
8.4 Modes of encryption 173
8.5 Exploring modes of encryption 178
8.6 The Data Encryption Standard 182
8.7 Feistel ciphers 182

8.8 Simplified DES: sDES . . . 183
8.9 The DES algorithm . . . 190
8.10 Security of S-boxes . . . 196
8.11 Security of DES . . . 204
8.12 Using DES . . . 205
8.13 Experimenting with DES . . . 206
8.14 Lightweight ciphers . . . 207
8.15 Glossary . . . 211
Exercises . . . 212

9 Finite fields **215**
9.1 Groups and rings . . . 215
9.2 Introduction to fields . . . 219
9.3 Fundamental algebra of finite fields . . . 222
9.4 Polynomials mod 2 . . . 224
9.5 A field of order 8 . . . 226
9.6 Other fields $GF(2^n)$ . . . 229
9.7 Multiplication and inversion . . . 230
9.8 Multiplication without power tables . . . 234
9.9 Glossary . . . 238
Exercises . . . 238

10 The Advanced Encryption Standard **245**
10.1 Introduction and some history . . . 245
10.2 Basic structure . . . 246
10.3 The layers in detail . . . 248
10.4 Decryption . . . 252
10.5 Experimenting with AES . . . 256
10.6 A simplified Rijndael . . . 258
10.7 Security of the AES . . . 264
10.8 Glossary . . . 265
Exercises . . . 265

11 Hash functions **267**
11.1 Uses of hash functions . . . 268
11.2 Security of hash functions . . . 270
11.3 Constructing a hash function . . . 271
11.4 Provably secure hash functions . . . 281
11.5 New hash functions . . . 285
11.6 Message authentication codes . . . 287
11.7 Using a MAC . . . 288
11.8 Glossary . . . 289
Exercises . . . 289

12 Elliptic curves and cryptosystems **295**
12.1 Basic definitions . . . 295

12.2 The group on an elliptic curve 300
12.3 Background and history 307
12.4 Multiplication 308
12.5 Elliptic curve cryptosystems 309
12.6 Elliptic curve signature schemes 316
12.7 Elliptic curves over binary fields 317
12.8 Pairing-based cryptography 318
12.9 Exploring pairings in Sage 323
12.10 Glossary 326
Exercises 327

13 Random numbers and stream ciphers **333**
13.1 Introduction 333
13.2 Pseudo-random number generators 334
13.3 Some cryptographically strong generators 338
13.4 The shrinking generator 341
13.5 ISAAC and Fortuna 344
13.6 Stream ciphers 346
13.7 RC4 348
13.8 The Blum–Goldwasser cryptosystem 351
13.9 Glossary 355
Exercises 356

14 Advanced applications and protocols **361**
14.1 Secure multi-party computation 361
14.2 Zero knowledge proofs 366
14.3 Oblivious transfer 371
14.4 Digital cash 374
14.5 Voting protocols 382
14.6 Glossary 388
Exercises 389

Appendix A Introduction to Sage **395**
A.1 Obtaining and installing Sage 395
A.2 Starting with Sage 396
A.3 Basic usage 396
A.4 Tab completion and help 402
A.5 Basic programming 404
A.6 A programming example 407
Exercises 408

Appendix B Advanced computational number theory **411**
B.1 The quadratic sieve 411
B.2 The AKS primality test 415
B.3 Methods of computing discrete logarithms 417
Exercises 423

Bibliography 425

Index 435

Computer Science

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

Once the privilege of a secret few, cryptography is now taught at universities around the world. **Introduction to Cryptography with Open-Source Software** illustrates algorithms and cryptosystems using examples and the open-source computer algebra system of Sage. The author, a noted educator in the field, provides a highly practical learning experience by progressing at a gentle pace, keeping mathematics at a manageable level, and including numerous end-of-chapter exercises.

Focusing on the cryptosystems themselves rather than the means of breaking them, the book first explores when and how the methods of modern cryptography can be used and misused. It then presents number theory and the algorithms and methods that make up the basis of cryptography today. After a brief review of "classical" cryptography, the book introduces information theory and examines the public-key cryptosystems of RSA and Rabin's cryptosystem. Other public-key systems studied include the El Gamal cryptosystem, systems based on knapsack problems, and algorithms for creating digital signature schemes.

The second half of the text moves on to consider bit-oriented secret-key, or symmetric, systems suitable for encrypting large amounts of data. The author describes block ciphers (including the Data Encryption Standard), cryptographic hash functions, finite fields, the Advanced Encryption Standard, cryptosystems based on elliptical curves, random number generation, and stream ciphers. The book concludes with a look at examples and applications of modern cryptographic systems, such as multi-party computation, zero-knowledge proofs, oblivious transfer, and voting protocols.

CRC Press
Taylor & Francis Group
an informa business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K11232

ISBN: 978-1-4398-2570-9
90000
9 781439 825709