

Contents

| | |
|--|-----------|
| Preface | ix |
| 1 Overview of Cryptography and Its Applications | 1 |
| 1.1 Secure Communications | 2 |
| 1.2 Cryptographic Applications | 8 |
| 2 Classical Cryptosystems | 10 |
| 2.1 Shift Ciphers | 11 |
| 2.2 Affine Ciphers | 12 |
| 2.3 The Vigenère Cipher | 14 |
| 2.4 Substitution Ciphers | 20 |
| 2.5 Sherlock Holmes | 23 |
| 2.6 The Playfair and ADFGX Ciphers | 26 |
| 2.7 Enigma | 29 |
| 2.8 Exercises | 33 |
| 2.9 Computer Problems | 37 |
| 3 Basic Number Theory | 40 |
| 3.1 Basic Notions | 40 |
| 3.2 The Extended Euclidean Algorithm | 44 |
| 3.3 Congruences | 47 |
| 3.4 The Chinese Remainder Theorem | 52 |
| 3.5 Modular Exponentiation | 54 |
| 3.6 Fermat's Theorem and Euler's Theorem | 55 |
| 3.7 Primitive Roots | 59 |
| 3.8 Inverting Matrices Mod n | 61 |
| 3.9 Square Roots Mod n | 62 |
| 3.10 Legendre and Jacobi Symbols | 64 |
| 3.11 Finite Fields | 69 |
| 3.12 Continued Fractions | 76 |
| 3.13 Exercises | 78 |
| 3.14 Computer Problems | 86 |
| 4 The One-Time Pad | 88 |
| 4.1 Binary Numbers and ASCII | 88 |
| 4.2 One-Time Pads | 89 |
| 4.3 Multiple Use of a One-Time Pad | 91 |
| 4.4 Perfect Secrecy of the One-Time Pad | 94 |
| 4.5 Indistinguishability and Security | 97 |
| 4.6 Exercises | 100 |

| | | |
|-----------|---|------------|
| 5 | Stream Ciphers | 104 |
| 5.1 | Pseudorandom Bit Generation | 105 |
| 5.2 | LFSR Sequences | 107 |
| 5.3 | RC4 | 113 |
| 5.4 | Exercises | 114 |
| 5.5 | Computer Problems | 117 |
| 6 | Block Ciphers | 118 |
| 6.1 | Block Ciphers | 118 |
| 6.2 | Hill Ciphers | 119 |
| 6.3 | Modes of Operation | 122 |
| 6.4 | Multiple Encryption | 129 |
| 6.5 | Meet-in-the-Middle Attacks | 130 |
| 6.6 | Exercises | 131 |
| 6.7 | Computer Problems | 135 |
| 7 | The Data Encryption Standard | 136 |
| 7.1 | Introduction | 136 |
| 7.2 | A Simplified DES-Type Algorithm | 137 |
| 7.3 | Differential Cryptanalysis | 140 |
| 7.4 | DES | 145 |
| 7.5 | Breaking DES | 152 |
| 7.6 | Password Security | 155 |
| 7.7 | Exercises | 157 |
| 7.8 | Computer Problems | 159 |
| 8 | The Advanced Encryption Standard: Rijndael | 160 |
| 8.1 | The Basic Algorithm | 160 |
| 8.2 | The Layers | 161 |
| 8.3 | Decryption | 166 |
| 8.4 | Design Considerations | 168 |
| 8.5 | Exercises | 169 |
| 9 | The RSA Algorithm | 171 |
| 9.1 | The RSA Algorithm | 171 |
| 9.2 | Attacks on RSA | 177 |
| 9.3 | Primality Testing | 183 |
| 9.4 | Factoring | 188 |
| 9.5 | The RSA Challenge | 192 |
| 9.6 | An Application to Treaty Verification | 194 |
| 9.7 | The Public Key Concept | 195 |
| 9.8 | Exercises | 197 |
| 9.9 | Computer Problems | 207 |
| 10 | Discrete Logarithms | 211 |
| 10.1 | Discrete Logarithms | 211 |
| 10.2 | Computing Discrete Logs | 212 |
| 10.3 | Bit Commitment | 218 |
| 10.4 | Diffie-Hellman Key Exchange | 219 |
| 10.5 | The ElGamal Public Key Cryptosystem | 221 |
| 10.6 | Exercises | 223 |

| | | |
|-----------|---|------------|
| 10.7 | Computer Problems | 225 |
| 11 | Hash Functions | 226 |
| 11.1 | Hash Functions | 226 |
| 11.2 | Simple Hash Examples | 230 |
| 11.3 | The Merkle-Damgård Construction | 231 |
| 11.4 | SHA-2 | 233 |
| 11.5 | SHA-3/Keccak | 237 |
| 11.6 | Exercises | 242 |
| 12 | Hash Functions: Attacks and Applications | 246 |
| 12.1 | Birthday Attacks | 246 |
| 12.2 | Multicollisions | 249 |
| 12.3 | The Random Oracle Model | 251 |
| 12.4 | Using Hash Functions to Encrypt | 253 |
| 12.5 | Message Authentication Codes | 255 |
| 12.6 | Password Protocols | 256 |
| 12.7 | Blockchains | 262 |
| 12.8 | Exercises | 264 |
| 12.9 | Computer Problems | 268 |
| 13 | Digital Signatures | 269 |
| 13.1 | RSA Signatures | 270 |
| 13.2 | The ElGamal Signature Scheme | 271 |
| 13.3 | Hashing and Signing | 273 |
| 13.4 | Birthday Attacks on Signatures | 274 |
| 13.5 | The Digital Signature Algorithm | 275 |
| 13.6 | Exercises | 276 |
| 13.7 | Computer Problems | 281 |
| 14 | What Can Go Wrong | 282 |
| 14.1 | An Enigma “Feature” | 282 |
| 14.2 | Choosing Primes for RSA | 283 |
| 14.3 | WEP | 284 |
| 14.4 | Exercises | 288 |
| 15 | Security Protocols | 290 |
| 15.1 | Intruders-in-the-Middle and Impostors | 290 |
| 15.2 | Key Distribution | 293 |
| 15.3 | Kerberos | 299 |
| 15.4 | Public Key Infrastructures (PKI) | 303 |
| 15.5 | X.509 Certificates | 304 |
| 15.6 | Pretty Good Privacy | 309 |
| 15.7 | SSL and TLS | 312 |
| 15.8 | Secure Electronic Transaction | 314 |
| 15.9 | Exercises | 316 |

| | |
|--|------------|
| 16 Digital Cash | 318 |
| 16.1 Setting the Stage for Digital Economies | 319 |
| 16.2 A Digital Cash System | 320 |
| 16.3 Bitcoin Overview | 326 |
| 16.4 Cryptocurrencies | 329 |
| 16.5 Exercises | 338 |
| 17 Secret Sharing Schemes | 340 |
| 17.1 Secret Splitting | 340 |
| 17.2 Threshold Schemes | 341 |
| 17.3 Exercises | 346 |
| 17.4 Computer Problems | 348 |
| 18 Games | 349 |
| 18.1 Flipping Coins over the Telephone | 349 |
| 18.2 Poker over the Telephone | 351 |
| 18.3 Exercises | 355 |
| 19 Zero-Knowledge Techniques | 357 |
| 19.1 The Basic Setup | 357 |
| 19.2 The Feige-Fiat-Shamir Identification Scheme | 359 |
| 19.3 Exercises | 361 |
| 20 Information Theory | 365 |
| 20.1 Probability Review | 365 |
| 20.2 Entropy | 367 |
| 20.3 Huffman Codes | 371 |
| 20.4 Perfect Secrecy | 373 |
| 20.5 The Entropy of English | 376 |
| 20.6 Exercises | 380 |
| 21 Elliptic Curves | 384 |
| 21.1 The Addition Law | 384 |
| 21.2 Elliptic Curves Mod p | 389 |
| 21.3 Factoring with Elliptic Curves | 393 |
| 21.4 Elliptic Curves in Characteristic 2 | 396 |
| 21.5 Elliptic Curve Cryptosystems | 399 |
| 21.6 Exercises | 402 |
| 21.7 Computer Problems | 407 |
| 22 Pairing-Based Cryptography | 409 |
| 22.1 Bilinear Pairings | 409 |
| 22.2 The MOV Attack | 410 |
| 22.3 Tripartite Diffie-Hellman | 411 |
| 22.4 Identity-Based Encryption | 412 |
| 22.5 Signatures | 414 |
| 22.6 Keyword Search | 417 |
| 22.7 Exercises | 419 |

| | |
|---|------------|
| 23 Lattice Methods | 421 |
| 23.1 Lattices | 421 |
| 23.2 Lattice Reduction | 422 |
| 23.3 An Attack on RSA | 426 |
| 23.4 NTRU | 429 |
| 23.5 Another Lattice-Based Cryptosystem | 433 |
| 23.6 Post-Quantum Cryptography? | 435 |
| 23.7 Exercises | 435 |
| 24 Error Correcting Codes | 437 |
| 24.1 Introduction | 437 |
| 24.2 Error Correcting Codes | 442 |
| 24.3 Bounds on General Codes | 446 |
| 24.4 Linear Codes | 451 |
| 24.5 Hamming Codes | 457 |
| 24.6 Golay Codes | 459 |
| 24.7 Cyclic Codes | 466 |
| 24.8 BCH Codes | 472 |
| 24.9 Reed-Solomon Codes | 479 |
| 24.10 The McEliece Cryptosystem | 480 |
| 24.11 Other Topics | 483 |
| 24.12 Exercises | 483 |
| 24.13 Computer Problems | 487 |
| 25 Quantum Techniques in Cryptography | 488 |
| 25.1 A Quantum Experiment | 488 |
| 25.2 Quantum Key Distribution | 491 |
| 25.3 Shor's Algorithm | 493 |
| 25.4 Exercises | 502 |
| A Mathematica® Examples | 503 |
| A.1 Getting Started with Mathematica | 503 |
| A.2 Some Commands | 504 |
| A.3 Examples for Chapter 2 | 505 |
| A.4 Examples for Chapter 3 | 508 |
| A.5 Examples for Chapter 5 | 511 |
| A.6 Examples for Chapter 6 | 513 |
| A.7 Examples for Chapter 9 | 514 |
| A.8 Examples for Chapter 10 | 520 |
| A.9 Examples for Chapter 12 | 521 |
| A.10 Examples for Chapter 17 | 521 |
| A.11 Examples for Chapter 18 | 522 |
| A.12 Examples for Chapter 21 | 523 |
| B Maple® Examples | 527 |
| B.1 Getting Started with Maple | 527 |
| B.2 Some Commands | 528 |
| B.3 Examples for Chapter 2 | 529 |
| B.4 Examples for Chapter 3 | 533 |
| B.5 Examples for Chapter 5 | 536 |

| | | |
|----------|--|------------|
| B.6 | Examples for Chapter 6 | 538 |
| B.7 | Examples for Chapter 9 | 539 |
| B.8 | Examples for Chapter 10 | 546 |
| B.9 | Examples for Chapter 12 | 547 |
| B.10 | Examples for Chapter 17 | 548 |
| B.11 | Examples for Chapter 18 | 549 |
| B.12 | Examples for Chapter 21 | 551 |
| C | MATLAB® Examples | 555 |
| C.1 | Getting Started with MATLAB | 556 |
| C.2 | Examples for Chapter 2 | 560 |
| C.3 | Examples for Chapter 3 | 566 |
| C.4 | Examples for Chapter 5 | 569 |
| C.5 | Examples for Chapter 6 | 571 |
| C.6 | Examples for Chapter 9 | 573 |
| C.7 | Examples for Chapter 10 | 581 |
| C.8 | Examples for Chapter 12 | 581 |
| C.9 | Examples for Chapter 17 | 582 |
| C.10 | Examples for Chapter 18 | 582 |
| C.11 | Examples for Chapter 21 | 585 |
| D | Sage Examples | 591 |
| D.1 | Computations for Chapter 2 | 591 |
| D.2 | Computations for Chapter 3 | 594 |
| D.3 | Computations for Chapter 5 | 595 |
| D.4 | Computations for Chapter 6 | 596 |
| D.5 | Computations for Chapter 9 | 596 |
| D.6 | Computations for Chapter 10 | 597 |
| D.7 | Computations for Chapter 12 | 598 |
| D.8 | Computations for Chapter 17 | 598 |
| D.9 | Computations for Chapter 18 | 598 |
| D.10 | Computations for Chapter 21 | 599 |
| E | Answers and Hints for Selected Odd-Numbered Exercises | 601 |
| F | Suggestions for Further Reading | 607 |
| | Bibliography | 608 |
| | Index | 615 |