

Contents

| | | |
|----------|---|------------|
| 1 | Introduction | 13 |
| 2 | Basic cryptosystems | 19 |
| 2.1 | Goals of cryptography | 20 |
| 2.2 | Advanced Encryption Standard (AES) | 22 |
| 2.3 | The AES key schedule | 34 |
| 2.4 | Asymmetric vs. symmetric cryptography | 37 |
| 2.5 | The RSA cryptosystem | 38 |
| 2.6 | The Diffie-Hellman key exchange | 42 |
| 2.7 | Block ciphers | 48 |
| 2.8 | Stream ciphers and modes of operation | 50 |
| 2.9 | Secret sharing | 51 |
| 2.10 | Visual cryptography | 53 |
| | Notes | 54 |
| | Exercises | 56 |
| A | Classical cryptology | 61 |
| A.1 | Cryptographic primitives | 61 |
| A.2 | Brief history of cryptography | 69 |
| A.3 | Simple substitutions | 85 |
| A.4 | Frequency analysis | 87 |
| A.5 | Information theory | 95 |
| | Notes | 103 |
| | Exercises | 105 |
| 3 | The RSA cryptosystem | 109 |
| 3.1 | Analysis of RSA | 109 |
| 3.2 | Primality testing | 110 |
| 3.3 | Finding prime numbers | 118 |
| 3.4 | Finding safe prime numbers | 121 |
| 3.5 | Security of RSA | 123 |
| 3.6 | The Wiener attack | 127 |

| | | |
|----------|---|------------|
| 3.7 | Chinese remainder computation for RSA | 128 |
| 3.8 | Fault attacks | 129 |
| 3.9 | Hard core bit for RSA | 130 |
| 3.10 | Factoring integers | 131 |
| 3.11 | The birthday paradox | 132 |
| 3.12 | Pollard rho with Floyd's trick | 133 |
| 3.13 | Dixon's random squares | 136 |
| 3.14 | Factorization via element order | 140 |
| | Notes | 143 |
| | Exercises | 145 |
| B | Key addition and modular arithmetic | 157 |
| B.1 | Key addition systems | 157 |
| B.2 | Claude Comiers d'Ambrun | 159 |
| B.3 | Later work on arithmetic cryptography | 162 |
| | Notes | 167 |
| 4 | Group cryptography and discrete logarithms | 169 |
| 4.1 | Groups for cryptography | 169 |
| 4.2 | The ElGamal encryption scheme | 174 |
| 4.3 | Baby-step giant-step algorithm | 176 |
| 4.4 | The birthday attack | 178 |
| 4.5 | The Pollard rho algorithm | 179 |
| 4.6 | Chinese distribution of discrete logarithms | 184 |
| 4.7 | The Pohlig-Hellman algorithm | 188 |
| 4.8 | Index calculus | 191 |
| 4.9 | Arithmetic circuits for discrete logarithms | 194 |
| | Notes | 200 |
| | Exercises | 202 |
| 5 | Elliptic curves | 207 |
| 5.1 | Elliptic curves as groups | 207 |
| 5.2 | The geometric background | 213 |
| 5.3 | The size of an elliptic curve | 217 |
| 5.4 | Elliptic curve cryptography | 219 |
| 5.5 | Empirical cryptographic security | 222 |
| 5.6 | The NIST curves | 225 |
| 5.7 | Computing the size of an elliptic curve | 227 |
| 5.8 | Division polynomials | 230 |
| | Notes | 232 |
| | Exercises | 234 |

| | | |
|-----------|---|------------|
| C | Breaking the unbreakable | 241 |
| C.1 | Kasiski's attack on Vigenère | 241 |
| C.2 | Friedman's index of coincidence | 250 |
| C.3 | Polygram substitutions | 254 |
| C.4 | Polyalphabetic substitutions | 257 |
| Notes | | 258 |
| Exercises | | 259 |
| 6 | Differential and linear cryptanalysis | 263 |
| 6.1 | Baby-AES | 264 |
| 6.2 | Differential cryptanalysis | 268 |
| 6.3 | Linear cryptanalysis | 279 |
| 6.4 | Countermeasures and near-optimality of SUBBYTES | 290 |
| Notes | | 295 |
| Exercises | | 297 |
| 7 | Hash functions | 301 |
| 7.1 | Hash functions | 301 |
| 7.2 | A discrete logarithm hash function | 306 |
| 7.3 | Hashing long messages | 310 |
| 7.4 | Time stamps | 313 |
| 7.5 | The MD and SHA hash function families | 313 |
| 7.6 | The SHA-2 hash functions | 314 |
| Notes | | 314 |
| Exercises | | 316 |
| D | Codebooks | 321 |
| D.1 | Nomenclators 14th century | 321 |
| D.2 | Codebooks 15th century | 324 |
| D.3 | Codebooks 16th century | 326 |
| D.4 | Codebooks 18th century | 332 |
| D.5 | Commercial codebooks | 334 |
| D.6 | Unicity distance for codebooks | 335 |
| Notes | | 342 |
| Exercises | | 343 |
| 8 | Signatures | 347 |
| 8.1 | Digital signatures | 347 |
| 8.2 | ElGamal signatures | 349 |
| 8.3 | Forging ElGamal signatures | 351 |
| 8.4 | Schnorr signatures and the <i>Digital Signature Algorithm</i> | 353 |
| 8.5 | The Gennaro-Halevi-Rabin signature (GHR) scheme | 357 |

| | |
|--|------------|
| Notes | 359 |
| Exercises | 359 |
| 9 Security and reductions | 369 |
| 9.1 When can we consider a system “secure”? | 369 |
| 9.2 Security of encryption schemes | 373 |
| 9.3 One-way and trapdoor functions | 374 |
| 9.4 Perfect security: the one-time pad | 375 |
| 9.5 Taxonomy of security reductions for signatures | 377 |
| 9.6 Security of the GHR signature scheme | 380 |
| 9.7 Security reductions for encryption | 384 |
| 9.8 ElGamal encryption and decisional Diffie-Hellman | 389 |
| 9.9 Hofheinz-Kiltz-Shoup (HKS) encryption | 391 |
| 9.10 Security of HKS | 395 |
| Notes | 400 |
| Exercises | 403 |
| E Steganography | 409 |
| E.1 Invisible ink | 409 |
| E.2 Steganographic images | 414 |
| E.3 Bacon’s bilateral cipher | 414 |
| Notes | 416 |
| 10 Identification and authentication | 419 |
| 10.1 Identification schemes | 419 |
| 10.2 Schnorr identification scheme | 420 |
| 10.3 Okamoto identification scheme | 422 |
| 10.4 RSA-based identification | 425 |
| 10.5 Message authentication codes | 426 |
| 10.6 Authenticated key agreement | 428 |
| Notes | 429 |
| Exercises | 429 |
| F Transposition ciphers | 433 |
| F.1 The skytale tale | 433 |
| F.2 Columnar transpositions | 435 |
| F.3 Breaking a columnar transposition | 439 |
| F.4 Grilles | 440 |
| Notes | 442 |
| Exercises | 443 |

| | | |
|-----------|--|------------|
| 11 | Random generation | 447 |
| 11.1 | True random generators | 448 |
| 11.2 | Pseudorandom generators | 452 |
| 11.3 | Distinguishers | 456 |
| 11.4 | Predictors | 461 |
| 11.5 | From short to long generators | 470 |
| 11.6 | The Nisan-Wigderson generator | 474 |
| 11.7 | Construction of good designs | 478 |
| 11.8 | The Blum-Blum-Shub generator | 479 |
| | Notes | 489 |
| | Exercises | 490 |
| G | Some cryptographers | 499 |
| G.1 | Arab cryptology | 499 |
| G.2 | Cicco Simonetta | 503 |
| G.3 | Johannes Trithemius | 504 |
| G.4 | Marin Mersenne | 520 |
| G.5 | Athanasius Kircher and Kaspar Schott | 521 |
| G.6 | John Wallis | 523 |
| | Notes | 524 |
| 12 | Proof systems and zero knowledge | 529 |
| 12.1 | Interactive proof systems | 530 |
| 12.2 | Zero knowledge | 535 |
| 12.3 | Bit commitment | 543 |
| 12.4 | Computational zero knowledge | 545 |
| | Notes | 549 |
| | Exercises | 550 |
| H | People using cryptography | 555 |
| H.1 | Interception, Black Cabinets, and Martin Luther | 555 |
| H.2 | Hernán Cortés | 556 |
| H.3 | Margaret Kennedy | 559 |
| H.4 | Christopher Layer | 563 |
| H.5 | José Martí | 571 |
| | Notes | 572 |
| 13 | Integral lattices | 575 |
| 13.1 | Lattices and short vectors | 575 |
| 13.2 | Lenstra, Lenstra & Lovász' lattice basis reduction | 578 |
| 13.3 | Cost estimate for basis reduction | 582 |
| 13.4 | Breaking subset sum cryptosystems | 588 |

| | | |
|-----------|---|------------|
| 13.5 | Truncated linear congruential pseudorandom generators | 595 |
| 13.6 | Close vectors | 604 |
| 13.7 | The hidden number problem | 609 |
| 13.8 | Security of Diffie-Hellman | 613 |
| 13.9 | The Coppersmith method | 616 |
| 13.10 | Security of leading bits of an RSA prime | 621 |
| 13.11 | Security of leading bits of a secret CRT-RSA exponent | 623 |
| 13.12 | The complexity of short vector problems | 625 |
| 13.13 | Lattice cryptography: the Regev cryptosystem | 627 |
| | Notes | 648 |
| | Exercises | 651 |
| I | The Zimmermann telegram | 661 |
| I.1 | Capturing the <i>Magdeburg</i> 's codebooks | 661 |
| I.2 | The telegram | 664 |
| I.3 | Transmission and cryptanalysis | 669 |
| I.4 | The drama unfolds | 674 |
| | Notes | 677 |
| 14 | Quantum computation | 681 |
| 14.1 | Qubits | 681 |
| 14.2 | Quantum circuits | 687 |
| 14.3 | The quantum Fourier transform | 694 |
| 14.4 | Polynomial-time integer factorization | 699 |
| 14.5 | Discrete logarithms | 707 |
| 14.6 | Outlook on quantum computation | 712 |
| | Notes | 714 |
| | Exercises | 715 |
| J | ENIGMA, Turing, and COLOSSUS | 719 |
| J.1 | ENIGMA | 719 |
| J.2 | Bletchley Park | 725 |
| J.3 | Rotor cryptanalysis | 728 |
| | Notes | 733 |
| | Exercises | 736 |
| 15 | The computer algebra toolbox | 741 |
| 15.1 | Addition and multiplication | 743 |
| 15.2 | Homomorphisms and permutations | 746 |
| 15.3 | Division with remainder | 748 |
| 15.4 | The Extended Euclidean Algorithm | 750 |
| 15.5 | Modular inverses | 755 |

| | | |
|--|---|------------|
| 15.6 | Cost of algorithms and complexity of problems | 757 |
| 15.7 | Worst case vs. average case | 760 |
| 15.8 | The cost of arithmetic | 761 |
| 15.9 | Uniqueness of rational approximations | 763 |
| 15.10 | Polynomial interpolation | 765 |
| 15.11 | The Chinese Remainder Algorithm | 766 |
| 15.12 | Efficient exponentiation | 770 |
| 15.13 | Fermat, Euler, and Lagrange | 772 |
| 15.14 | Squares and the Jacobi symbol | 780 |
| 15.15 | Linear algebra | 785 |
| 15.16 | Finite probability spaces | 788 |
| | Notes | 796 |
| | Exercises | 799 |
| Notation and sources of quotations, images, and ornaments | | 807 |
| | Notation | 807 |
| | Sources of quotations | 808 |
| | Sources of images | 815 |
| | Sources of ornaments | 817 |
| Bibliography | | 819 |
| Index | | 863 |

By this contrivance, the most ignorant person, at a reasonable charge, and with a little bodily labor, may write books in philosophy, poetry, politics, law, mathematics, and theology, without the least assistance from genius or study.

JONATHAN SWIFT (1726)

'Tis pleasant sure to see one's name in print;
A Book's a Book, altho' there's nothing in't.

LORD BYRON (1809)

In these cursory observations we have by no means attempted to exhaust the subject of Cryptography. With such object in view, a folio might be required.

EDGAR ALLAN POE (1840)

Die Kunst stille zu schweigen, geneigter leser, ist gar ein edles Ding; noch edler aber wird meines Erachtens seyn die Kunst redend zu schweigen und solche lehret dich meine alhier in unserer Muttersprache an das Licht gegebene *Cryptographia*, oder Kunst verborgene Briefe und Schrifften zu machen.¹

JOHANNES BALTHASAR FRIDERICI (1685)

I went into the Army at Fort Devens in Massachusetts and was sorted into the Signal Corps, and so got in the Signal Corps training camp at Fort Monmouth in New Jersey. They took everybody who had no visible talent or aptitude whatsoever for electrical work, or communications in the technological sense, and if they had a certain level of testing score under the Army General Classification Test, bing! Crypt School before you could sneeze.

WILLIAM P. BUNDY (1987)

Will the study of cryptology become an epidemic that even all the government's resources will be unable to stem?

DAVID KAHN (1979)

¹The art of being quietly silent, estimated reader, is a truly noble thing; even nobler is in my view the art of being silent while talking, and this art is taught to you by my *Cryptographia*, or the art of making hidden letters and writings, brought here to the light of day in our mother tongue.



<http://www.springer.com/978-3-662-48423-4>

CryptoSchool

von zur Gathen, J.

2015, XII, 876 p. 186 illus., 97 illus. in color., Hardcover

ISBN: 978-3-662-48423-4