- Chapter 1 A History of Cryptography p. 1
- 1.1 Codes p. 2
- 1.2 Monoalphabetic Substitution Ciphers p. 3
- 1.3 Frequency Analysis on Caesar Ciphers p. 4
- 1.4 Frequency Analysis on Monoalphabetic Substitution Ciphers p. 7
- 1.5 Polyalphabetic Substitution Ciphers p. 8
- 1.6 The Vigenere Cipher and Code Wheels p. 10
- 1.7 Breaking Simple Vigenere Ciphers p. 11
- 1.8 The Kaisiski Method of Determining Key Length p. 12
- 1.9 The Full Vigenere Cipher p. 14
- 1.10 The Auto-Key Vigenere Cipher p. 16
- 1.11 The Running Key Vigenere Cipher p. 17
- 1.12 Breaking Auto-Key and Running Key Vigenere Ciphers p. 18
- 1.13 The One-Time Pad p. 18
- 1.14 Transposition Ciphers p. 19
- 1.15 Polygram Substitution Ciphers p. 20
- 1.16 The Playfair Cipher p. 20
- 1.17 Breaking Simple Polygram Ciphers p. 23
- 1.18 The Jefferson Cylinder p. 23
- 1.19 Homophonic Substitution Ciphers p. 24
- 1.20 Combination Substitution/Transposition Ciphers p. 26
- Exercises p. 28
- Chapter 2 Large Integer Computing p. 33
- 2.1 Constructors p. 34
- 2.2 Comparison Methods p. 38
- 2.3 Arithmetic Methods p. 41
- 2.4 The Java BigInteger Class p. 51
- 2.5 Constructors p. 51
- 2.6 Methods p. 54
- Exercises p. 62
- Chapter 3 The Integers p. 65
- 3.1 The Division Algorithm p. 66
- 3.2 The Euclidean Algorithm p. 77
- 3.3 The Fundamental Theorem of Arithmetic p. 82
- Exercises p. 86
- Chapter 4 Linear Diophantine Equations and Linear Congruences p. 89
- 4.1 Linear Diophantine Equations p. 89
- 4.2 Linear Congruences p. 92
- 4.3 Modular Inverses p. 98
- Exercises p. 100
- Chapter 5 Linear Ciphers p. 105
- 5.1 The Caesar Cipher p. 105
- 5.2 Weaknesses of the Caesar Cipher p. 111
- 5.3 Affine Transformation Ciphers p. 111
- 5.4 Weaknesses of Affine Transformation Ciphers p. 113
- 5.5 The Vigenere Cipher p. 115

- 5.6 Block Affine Ciphers p. 116
- 5.7 Weaknesses of the Block Affine Cipher, Known Plaintext Attack p. 118
- 5.8 Padding Methods p. 119
- Exercises p. 124
- Chapter 6 Systems of Linear Congruences--Single Modulus p. 125
- 6.1 Modular Matrices p. 125
- 6.2 Modular Matrix Inverses p. 129
- Exercises p. 141
- Chapter 7 Matrix Ciphers p. 143
- 7.1 Weaknesses of Matrix Cryptosystems p. 144
- 7.2 Transposition Ciphers p. 150
- 7.3 Combination Substitution/Transposition Ciphers p. 154
- Exercises p. 159
- Chapter 8 Systems of Linear Congruences--Multiple Moduli p. 161
- 8.1 The Chinese Remainder Theorem p. 162
- Exercises p. 166
- Chapter 9 Quadratic Congruences p. 169
- 9.1 Quadratic Congruences Modulo a Prime p. 169
- 9.2 Fermat's Little Theorem p. 170
- 9.3 Quadratic Congruences Modulo a Composite p. 171
- Exercises p. 179
- Chapter 10 Quadratic Ciphers p. 181
- 10.1 The Rabin Cipher p. 181
- 10.2 Weaknesses of the Rabin Cipher p. 185
- 10.3 Strong Primes p. 190
- 10.4 Salt p. 199
- 10.5 Cipher Block Chaining (CBC) p. 204
- 10.6 Blum-Goldwasser Probabilistic Cipher p. 208
- 10.7 Weaknesses of the Blum-Goldwasser Probabilistic Cipher p. 211
- Exercises p. 212
- Chapter 11 Primality Testing p. 213
- 11.1 Miller's Test p. 215
- 11.2 The Rabin-Miller Test p. 217
- Exercises p. 219
- Chapter 12 Factorization Techniques p. 221
- 12.1 Fermat Factorization p. 221
- 12.2 Monte Carlo Factorization p. 226
- 12.3 The Pollard p-1 Method of Factorization p. 230
- Exercises p. 234
- Chapter 13 Exponential Congruences p. 235
- 13.1 Order of an Integer p. 236
- 13.2 Generators p. 237
- 13.3 Generator Selection p. 239
- 13.4 Calculating Discrete Logarithms p. 243
- Exercises p. 256
- Chapter 14 Exponential Ciphers p. 259

- 14.1 Diffie-Hellman Key Exchange p. 259
- 14.2 Weaknesses of Diffie-Hellman p. 260
- 14.3 The Pohlig-Hellman Exponentiation Cipher p. 260
- 14.4 Weaknesses of the Pohlig-Hellman Cipher p. 261
- 14.5 Cipher Feedback Mode (CFB) p. 262
- 14.6 The ElGamal Cipher p. 267
- 14.7 Weaknesses of ElGamal p. 269
- 14.8 The RSA Cipher p. 270
- 14.9 Weaknesses of RSA p. 272
- Exercises p. 278
- Chapter 15 Establishing Keys and Message Exchange p. 279
- 15.1 Establishing Keys p. 279
- 15.2 Diffie-Hellman Key Exchange Application p. 281
- 15.3 Message Exchange p. 284
- 15.4 Cipher Chat Application p. 284
- Exercises p. 298
- Chapter 16 Cryptographic Applications p. 299
- 16.1 Shadows p. 299
- 16.2 Database Encryption p. 306
- 16.3 Large Integer Arithmetic p. 309
- 16.4 Random Number Generation p. 315
- 16.5 Signing Messages p. 320
- 16.6 Message Digests p. 326
- 16.7 Signing with ElGamal p. 334
- 16.8 Attacks on Digest Functions p. 338
- 16.9 Zero Knowledge Identification p. 340
- Exercises p. 350
- Appendix List of Propositions p. 351
- Appendix II Information Theory p. 357
- AII.1 Entropy of a Message p. 357
- AII.2 Rate of a Language p. 358
- AII.3 Cryptographic Techniques p. 360
- AII.4 Confusion p. 360
- AII.5 Diffusion p. 361
- AII.6 Compression p. 361
- Recommended Reading p. 365
- Index p. 367