

Introduction to

Cryptography

with Java™ Applets

David Bishop

JONES AND BARTLETT COMPUTER SCIENCE

Contents

Chapter 1: A History of Cryptography 1

- 1.1 Codes 2
- 1.2 Monoalphabetic Substitution Ciphers 3
- 1.3 Frequency Analysis on Caesar Ciphers 4
- 1.4 Frequency Analysis on Monoalphabetic Substitution Ciphers 7
- 1.5 Polyalphabetic Substitution Ciphers 8
- 1.6 The Vigenere Cipher and Code Wheels 10
- 1.7 Breaking Simple Vigenere Ciphers 11
- 1.8 The Kaisiski Method of Determining Key Length 12
- 1.9 The Full Vigenere Cipher 14
- 1.10 The Auto-Key Vigenere Cipher 16
- 1.11 The Running Key Vigenere Cipher 17
- 1.12 Breaking Auto-Key and Running Key Vigenere Ciphers 18
- 1.13 The One-Time Pad 18
- 1.14 Transposition Ciphers 19
- 1.15 Polygram Substitution Ciphers 20
- 1.16 The Playfair Cipher 20
- 1.17 Breaking Simple Polygram Ciphers 23
- 1.18 The Jefferson Cylinder 23
- 1.19 Homophonic Substitution Ciphers 24
- 1.20 Combination Substitution/Transposition Ciphers 26
- Exercises 28

Chapter 2: Large Integer Computing 33

- 2.1 Constructors 34
- 2.2 Comparison Methods 38
- 2.3 Arithmetic Methods 41
- 2.4 The Java BigInteger Class 51
- 2.5 Constructors 51

xiv Contents

- 2.6 Methods 54
- Exercises 62

Chapter 3: The Integers 65

- 3.1 The Division Algorithm 66
- 3.2 The Euclidean Algorithm 77
- 3.3 The Fundamental Theorem of Arithmetic 82
- Exercises 86

Chapter 4: Linear Diophantine Equations and Linear Congruences 89

- 4.1 Linear Diophantine Equations 89
- 4.2 Linear Congruences 92
- 4.3 Modular Inverses 98
- Exercises 100

Chapter 5: Linear Ciphers 105

- 5.1 The Caesar Cipher 105
- 5.2 Weaknesses of the Caesar Cipher 111
- 5.3 Affine Transformation Ciphers 111
- 5.4 Weaknesses of Affine Transformation Ciphers 113
- 5.5 The Vigenere Cipher 115
- 5.6 Block Affine Ciphers 116
- 5.7 Weaknesses of the Block Affine Cipher, Known Plaintext Attack 118
- 5.8 Padding Methods 119
- Exercises 124

Chapter 6: Systems of Linear Congruences—Single Modulus 125

- 6.1 Modular Matrices 125
- 6.2 Modular Matrix Inverses 129
- Exercises 141

Chapter 7: Matrix Ciphers 143

- 7.1 Weaknesses of Matrix Cryptosystems 144
- 7.2 Transposition Ciphers 150
- 7.3 Combination Substitution/Transposition Ciphers 154
- Exercises 159

Chapter 8: Systems of Linear Congruences—Multiple Moduli 161

- 8.1 The Chinese Remainder Theorem 162
- Exercises 166

Chapter 9: Quadratic Congruences 169

- 9.1 Quadratic Congruences Modulo a Prime 169
- 9.2 Fermat's Little Theorem 170
- 9.3 Quadratic Congruences Modulo a Composite 171
- Exercises 179

Chapter 10: Quadratic Ciphers 181

- 10.1 The Rabin Cipher 181
- 10.2 Weaknesses of the Rabin Cipher 185
- 10.3 *Strong Primes* 190
- 10.4 Salt 199
- 10.5 Cipher Block Chaining (CBC) 204
- 10.6 Blum–Goldwasser Probabilistic Cipher 208
- 10.7 Weaknesses of the Blum–Goldwasser Probabilistic Cipher 211
- Exercises 212

Chapter 11: Primality Testing 213

- 11.1 Miller's Test 215
- 11.2 The Rabin–Miller Test 217
- Exercises 219

Chapter 12: Factorization Techniques 221

- 12.1 Fermat Factorization 221
- 12.2 Monte Carlo Factorization 226
- 12.3 The Pollard $p-1$ Method of Factorization 230
- Exercises 234

Chapter 13: Exponential Congruences 235

- 13.1 Order of an Integer 236
- 13.2 Generators 237
- 13.3 Generator Selection 239
- 13.4 Calculating Discrete Logarithms 243
- Exercises 256

Chapter 14: Exponential Ciphers 259

- 14.1 Diffie–Hellman Key Exchange 259
- 14.2 Weaknesses of Diffie–Hellman 260
- 14.3 The Pohlig–Hellman Exponentiation Cipher 260
- 14.4 Weaknesses of the Pohlig–Hellman Cipher 261
- 14.5 Cipher Feedback Mode (CFB) 262
- 14.6 The ElGamal Cipher 267
- 14.7 Weaknesses of ElGamal 269

xvi Contents

- 14.8 The RSA Cipher 270
- 14.9 Weaknesses of RSA 272
- Exercises 278

Chapter 15: Establishing Keys and Message Exchange 279

- 15.1 Establishing Keys 279
- 15.2 Diffie–Hellman Key Exchange Application 281
- 15.3 Message Exchange 284
- 15.4 Cipher Chat Application 284
- Exercises 298

Chapter 16: Cryptographic Applications 299

- 16.1 Shadows 299
- 16.2 Database Encryption 306
- 16.3 Large Integer Arithmetic 309
- 16.4 Random Number Generation 315
- 16.5 Signing Messages 320
- 16.6 Message Digests 326
- 16.7 Signing with ElGamal 334
- 16.8 Attacks on Digest Functions 338
- 16.9 Zero Knowledge Identification 340
- Exercises 350

Appendix: List of Propositions 351

Appendix II: Information Theory 357

- AII.1 Entropy of a Message 357
- AII.2 Rate of a Language 358
- AII.3 Cryptographic Techniques 360
- AII.4 Confusion 360
- AII.5 Diffusion 361
- AII.6 Compression 361
- Recommended Reading 365

Index 367