

COMPUTATIONAL MATHEMATICS SERIES

CRYPTANALYSIS of NUMBER THEORETIC CIPHERS

Samuel S. Wagstaff, Jr.



CHAPMAN & HALL/CRC

A CRC Press Company

Boca Raton London New York Washington, D.C.

Contents

I	Mathematical Foundations of Cryptanalysis	1
1	Terminology of Cryptography	3
1.1	Notation	3
1.2	Types of Attacks	4
1.3	Public Key Ciphers	6
1.4	Block and Stream Ciphers	7
1.5	Protocols	10
1.6	Exercises	10
2	Probability Theory	13
2.1	Definitions	13
2.2	The Birthday Problem	15
2.3	Random Variables	20
2.4	Exercises	24
3	Divisibility and Arithmetic	27
3.1	Divisibility	27
3.2	Arithmetic with Large Integers	28
3.3	Greatest Common Divisors and the Euclidean Algorithm	36
3.4	Exercises	42
4	Primes	45
4.1	The Fundamental Theorem of Arithmetic	45
4.2	The Distribution of Prime Numbers	49
4.3	Identifying and Finding Primes	51
4.4	The Largest Prime Factor of a Number	54
4.5	Exercises	59
5	Congruences	61
5.1	Simple Properties of Congruences	61
5.2	Linear Congruences	64
5.3	The Chinese Remainder Theorem	69
5.4	Exercises	72

- 6 Euler’s Theorem and Its Consequences 75**
 - 6.1 Fermat’s Little Theorem 75
 - 6.2 Euler’s Theorem 79
 - 6.3 Primitive Roots 86
 - 6.4 Discrete Logarithms 89
 - 6.5 Exercises 91

- 7 Second Degree Congruences 93**
 - 7.1 The Legendre Symbol 94
 - 7.2 The Law of Quadratic Reciprocity 98
 - 7.3 The Jacobi Symbol 100
 - 7.4 Euler Pseudoprimes 103
 - 7.5 Solving Quadratic Congruences Modulo m 104
 - 7.6 Exercises 110

- 8 Information Theory 111**
 - 8.1 Entropy 111
 - 8.2 Perfect Secrecy 114
 - 8.3 Unicity Distance 115
 - 8.4 Some Obsolete Ciphers 117
 - 8.5 The Entropy of Number Theoretic Ciphers 121
 - 8.6 Exercises 122

- 9 Groups, Rings and Fields 125**
 - 9.1 Groups 125
 - 9.2 Simple Properties of Groups 127
 - 9.3 The Baby-Step-Giant-Step Algorithm 130
 - 9.4 Rings and Fields 132
 - 9.5 Polynomials 133
 - 9.6 Algebraic Number Theory 137
 - 9.7 Exercises 140

- 10 Exponential Methods of Factoring Integers 143**
 - 10.1 Fermat’s Difference of Squares Method 143
 - 10.2 Pollard’s Rho Method 146
 - 10.3 Pollard’s $p - 1$ Method 149
 - 10.4 Square Form Factorization 151
 - 10.5 Exercises 153

- 11 Finding Large Primes 155**
 - 11.1 Stronger Probable Prime Tests 156
 - 11.2 Lucas Probable Prime Tests 160
 - 11.3 Rigorous Proof of Primality 165
 - 11.4 Prime Proofs for Arbitrary Large Integers 169
 - 11.5 Exercises 169

12 Elliptic Curves	171
12.1 Definitions and Examples	171
12.2 Factoring with Elliptic Curves	176
12.3 Primality Proving with Elliptic Curves	181
12.4 Exercises	182
13 Subexponential Factoring Algorithms	185
13.1 Factoring with Continued Fractions	185
13.2 The Quadratic Sieve	190
13.3 Variations of the Quadratic Sieve	193
13.3.1 Large Primes	193
13.3.2 Multiple Polynomials	194
13.3.3 The Self-Initializing Quadratic Sieve	195
13.4 The Number Field Sieve	196
13.5 Exercises	201
14 Computing Discrete Logarithms	203
14.1 Shanks' Baby-Step-Giant-Step Method	204
14.2 Pollard's Methods	204
14.2.1 The Rho Method for Discrete Logarithms	204
14.2.2 The Lambda Method for Discrete Logarithms	205
14.3 Discrete Logarithms via Index Calculus	206
14.4 Other Fast Methods for the Group R_m	207
14.5 Exercises	210
15 Random Number Generation	211
15.1 Linear Feedback Shift Registers	212
15.2 A Quadratic Residue Random Number Generator	215
15.3 Hash Functions	216
15.4 Generating Truly Random Numbers	217
15.5 Exercises	218
II The Cryptographic Algorithms	219
16 Private Key Ciphers	221
16.1 Rijndael, the Advanced Encryption Standard	221
16.1.1 Byte Arithmetic in Rijndael	222
16.1.2 Word Arithmetic in Rijndael	224
16.1.3 The Structure of Rijndael	225
16.1.4 The Key Schedule of Rijndael	227
16.1.5 Summary of Rijndael	227
16.2 The Pohlig-Hellman Cipher	228
16.3 Elliptic Curve Pohlig-Hellman	228
16.4 Exercises	230

17 Public Key Ciphers	231
17.1 Rivest-Shamir-Adleman	231
17.2 Massey-Omura	232
17.3 Elliptic Curve Massey-Omura	233
17.4 ElGamal	233
17.5 Elliptic Curve ElGamal	234
17.6 Rabin-Williams	235
17.7 Exercises	237
18 Signature Algorithms	239
18.1 Rivest-Shamir-Adleman Signatures	239
18.2 ElGamal Signatures	240
18.3 Rabin-Williams Signatures	241
18.4 The Digital Signature Algorithm	242
18.5 Exercises	244
19 Key Exchange Algorithms	245
19.1 Key Exchange Using a Trusted Server	245
19.2 The Diffie-Hellman Key Exchange	248
19.3 The X.509 Key Exchange	249
19.4 Exercises	251
20 Simple Protocols	253
20.1 Bit Commitment	253
20.2 Mental Poker	253
20.3 Oblivious Transfer	255
20.4 Zero-knowledge Proofs	256
20.5 Methods of Sharing Secrets	258
20.5.1 Secret Splitting	258
20.5.2 The Lagrange Interpolating Polynomial Scheme	258
20.5.3 The Asmuth and Bloom Threshold Scheme	260
20.6 Blind Signatures	261
20.7 Exercises	261
21 Complicated Protocols	263
21.1 Contract Signing	263
21.2 Secure Elections	265
21.3 Electronic Cash	268
21.3.1 Electronic Cash According to Chaum	268
21.3.2 Electronic Cash According to Brands	271
21.4 Exercises	274

22 Complete Systems **275**

- 22.1 Kerberos 275
- 22.2 Pretty Good Privacy 277
- 22.3 Exercises 278

III Methods of Attack **279**

23 Direct Attacks **281**

- 23.1 Try All Keys 281
- 23.2 Factor a Large Integer 283
- 23.3 Solve a Discrete Logarithm Problem 284
- 23.4 Timing Attacks 286
- 23.5 Exercises 287

24 Exploiting an Error **289**

- 24.1 Key Management 289
- 24.2 Reuse of a Key 290
- 24.3 Bad Parameter Choice 291
- 24.4 Partial Key Exposure 293
- 24.5 Computer Failure 293
- 24.6 Exercises 294

25 Active Attacks **297**

- 25.1 Force a User to Make a Mistake 297
- 25.2 Man-in-the-Middle Attacks 298
- 25.3 Birthday Attacks 300
- 25.4 Subliminal Channels 300
- 25.5 Exercises 301

References **303**

Index **311**