

Contents

Preface	v
Introduction	xiii
1 An Introduction to Cryptography	1
1.1 Simple Substitution Ciphers	1
1.1.1 Cryptanalysis of Simple Substitution Ciphers	4
1.2 Divisibility and Greatest Common Divisors	10
1.3 Modular Arithmetic	19
1.3.1 Modular Arithmetic and Shift Ciphers	23
1.3.2 The Fast Powering Algorithm	24
1.4 Prime Numbers, Unique Factorization, and Finite Fields	26
1.5 Powers and Primitive Roots in Finite Fields	29
1.6 Cryptography Before the Computer Age	34
1.7 Symmetric and Asymmetric Ciphers	37
1.7.1 Symmetric Ciphers	37
1.7.2 Encoding Schemes	39
1.7.3 Symmetric Encryption of Encoded Blocks	40
1.7.4 Examples of Symmetric Ciphers	41
1.7.5 Random Bit Sequences and Symmetric Ciphers	44
1.7.6 Asymmetric Ciphers Make a First Appearance	46
Exercises	47
2 Discrete Logarithms and Diffie–Hellman	61
2.1 The Birth of Public Key Cryptography	61
2.2 The Discrete Logarithm Problem	64
2.3 Diffie–Hellman Key Exchange	67
2.4 The Elgamal Public Key Cryptosystem	70
2.5 An Overview of the Theory of Groups	74
2.6 How Hard Is the Discrete Logarithm Problem?	77
2.7 A Collision Algorithm for the DLP	81
	vii

2.8	The Chinese Remainder Theorem	83
2.8.1	Solving Congruences with Composite Moduli	86
2.9	The Pohlig–Hellman Algorithm	88
2.10	Rings, Quotients, Polynomials, and Finite Fields	94
2.10.1	An Overview of the Theory of Rings	95
2.10.2	Divisibility and Quotient Rings	96
2.10.3	Polynomial Rings and the Euclidean Algorithm	98
2.10.4	Polynomial Ring Quotients and Finite Fields	102
	Exercises	107
3	Integer Factorization and RSA	117
3.1	Euler’s Formula and Roots Modulo pq	117
3.2	The RSA Public Key Cryptosystem	123
3.3	Implementation and Security Issues	126
3.4	Primality Testing	128
3.4.1	The Distribution of the Set of Primes	133
3.4.2	Primality Proofs Versus Probabilistic Tests	136
3.5	Pollard’s $p - 1$ Factorization Algorithm	137
3.6	Factorization via Difference of Squares	141
3.7	Smooth Numbers and Sieves	150
3.7.1	Smooth Numbers	150
3.7.2	The Quadratic Sieve	155
3.7.3	The Number Field Sieve	162
3.8	The Index Calculus and Discrete Logarithms	166
3.9	Quadratic Residues and Quadratic Reciprocity	169
3.10	Probabilistic Encryption	177
	Exercises	180
4	Digital Signatures	193
4.1	What Is a Digital Signature?	193
4.2	RSA Digital Signatures	196
4.3	Elgamal Digital Signatures and DSA	198
	Exercises	203
5	Combinatorics, Probability, and Information Theory	207
5.1	Basic Principles of Counting	208
5.1.1	Permutations	210
5.1.2	Combinations	211
5.1.3	The Binomial Theorem	213
5.2	The Vigenère Cipher	214
5.2.1	Cryptanalysis of the Vigenère Cipher: Theory	218
5.2.2	Cryptanalysis of the Vigenère Cipher: Practice	223
5.3	Probability Theory	228
5.3.1	Basic Concepts of Probability Theory	228

5.3.2	Bayes's Formula	233
5.3.3	Monte Carlo Algorithms	236
5.3.4	Random Variables	238
5.3.5	Expected Value	244
5.4	Collision Algorithms and Meet-in-the-Middle Attacks	246
5.4.1	The Birthday Paradox	246
5.4.2	A Collision Theorem	247
5.4.3	A Discrete Logarithm Collision Algorithm	250
5.5	Pollard's ρ Method	253
5.5.1	Abstract Formulation of Pollard's ρ Method	254
5.5.2	Discrete Logarithms via Pollard's ρ Method	259
5.6	Information Theory	263
5.6.1	Perfect Secrecy	263
5.6.2	Entropy	269
5.6.3	Redundancy and the Entropy of Natural Language	275
5.6.4	The Algebra of Secrecy Systems	277
5.7	Complexity Theory and $\mathcal{P}$ Versus $\mathcal{NP}$	278
	Exercises	282
6	Elliptic Curves and Cryptography	299
6.1	Elliptic Curves	299
6.2	Elliptic Curves over Finite Fields	306
6.3	The Elliptic Curve Discrete Logarithm Problem	310
6.3.1	The Double-and-Add Algorithm	312
6.3.2	How Hard Is the ECDLP?	315
6.4	Elliptic Curve Cryptography	316
6.4.1	Elliptic Diffie–Hellman Key Exchange	316
6.4.2	Elliptic Elgamal Public Key Cryptosystem	319
6.4.3	Elliptic Curve Signatures	321
6.5	The Evolution of Public Key Cryptography	321
6.6	Lenstra's Elliptic Curve Factorization Algorithm	324
6.7	Elliptic Curves over $\mathbb{F}_2$ and over $\mathbb{F}_{2^k}$	329
6.8	Bilinear Pairings on Elliptic Curves	336
6.8.1	Points of Finite Order on Elliptic Curves	337
6.8.2	Rational Functions and Divisors on Elliptic Curves	338
6.8.3	The Weil Pairing	340
6.8.4	An Efficient Algorithm to Compute the Weil Pairing	343
6.8.5	The Tate Pairing	346
6.9	The Weil Pairing over Fields of Prime Power Order	347
6.9.1	Embedding Degree and the MOV Algorithm	347
6.9.2	Distortion Maps and a Modified Weil Pairing	350
6.9.3	A Distortion Map on $y^2 = x^3 + x$	352

6.10 Applications of the Weil Pairing	356
6.10.1 Tripartite Diffie–Hellman Key Exchange	356
6.10.2 ID-Based Public Key Cryptosystems	358
Exercises	361
7 Lattices and Cryptography	373
7.1 A Congruential Public Key Cryptosystem	373
7.2 Subset-Sum Problems and Knapsack Cryptosystems	377
7.3 A Brief Review of Vector Spaces	384
7.4 Lattices: Basic Definitions and Properties	388
7.5 Short Vectors in Lattices	395
7.5.1 The Shortest and the Closest Vector Problems	395
7.5.2 Hermite’s Theorem and Minkowski’s Theorem	396
7.5.3 The Gaussian Heuristic	400
7.6 Babai’s Algorithm	403
7.7 Cryptosystems Based on Hard Lattice Problems	407
7.8 The GGH Public Key Cryptosystem	409
7.9 Convolution Polynomial Rings	412
7.10 The NTRU Public Key Cryptosystem	416
7.10.1 NTRUEncrypt	417
7.10.2 Mathematical Problems for NTRUEncrypt	422
7.11 NTRUEncrypt as a Lattice Cryptosystem	425
7.11.1 The NTRU Lattice	425
7.11.2 Quantifying the Security of an NTRU Lattice	427
7.12 Lattice-Based Digital Signature Schemes	428
7.12.1 The GGH Digital Signature Scheme	428
7.12.2 Transcript Analysis	430
7.12.3 Rejection Sampling	431
7.12.4 Rejection Sampling Applied to an Abstract Signature Scheme	433
7.12.5 The NTRU Modular Lattice Signature Scheme	434
7.13 Lattice Reduction Algorithms	436
7.13.1 Gaussian Lattice Reduction in Dimension 2	436
7.13.2 The LLL Lattice Reduction Algorithm	439
7.13.3 Using LLL to Solve apprCVP	448
7.13.4 Generalizations of LLL	449
7.14 Applications of LLL to Cryptanalysis	450
7.14.1 Congruential Cryptosystems	451
7.14.2 Applying LLL to Knapsacks	451
7.14.3 Applying LLL to GGH	452
7.14.4 Applying LLL to NTRU	453
Exercises	454

8 Additional Topics in Cryptography	471
8.1 Hash Functions	472
8.2 Random Numbers and Pseudorandom Number	474
8.3 Zero-Knowledge Proofs	477
8.4 Secret Sharing Schemes	480
8.5 Identification Schemes	481
8.6 Padding Schemes and the Random Oracle Model	482
8.7 Building Protocols from Cryptographic Primitives	485
8.8 Blind Digital Signatures, Digital Cash, and Bitcoin	487
8.9 Homomorphic Encryption	490
8.10 Hyperelliptic Curve Cryptography	494
8.11 Quantum Computing	497
8.12 Modern Symmetric Cryptosystems: DES and AES	499
 List of Notation	 503
 References	 507
 Index	 517