

# Contents

Preface	v
Introduction	xi
<b>1 An Introduction to Cryptography</b>	<b>1</b>
1.1 Simple substitution ciphers	1
1.2 Divisibility and greatest common divisors	10
1.3 Modular arithmetic	19
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	36
Exercises	47
<b>2 Discrete Logarithms and Diffie–Hellman</b>	<b>59</b>
2.1 The birth of public key cryptography	59
2.2 The discrete logarithm problem	62
2.3 Diffie–Hellman key exchange	65
2.4 The ElGamal public key cryptosystem	68
2.5 An overview of the theory of groups	72
2.6 How hard is the discrete logarithm problem?	75
2.7 A collision algorithm for the DLP	79
2.8 The Chinese remainder theorem	81
2.9 The Pohlig–Hellman algorithm	86
2.10 Rings, quotients, polynomials, and finite fields	92
Exercises	105
<b>3 Integer Factorization and RSA</b>	<b>113</b>
3.1 Euler’s formula and roots modulo $pq$	113
3.2 The RSA public key cryptosystem	119
3.3 Implementation and security issues	122
3.4 Primality testing	124
3.5 Pollard’s $p - 1$ factorization algorithm	133

3.6	Factorization via difference of squares . . . . .	137
3.7	Smooth numbers and sieves . . . . .	146
3.8	The index calculus and discrete logarithms . . . . .	162
3.9	Quadratic residues and quadratic reciprocity . . . . .	165
3.10	Probabilistic encryption . . . . .	172
	Exercises . . . . .	176
<b>4</b>	<b>Combinatorics, Probability, and Information Theory</b>	<b>189</b>
4.1	Basic principles of counting . . . . .	190
4.2	The Vigenère cipher . . . . .	196
4.3	Probability theory . . . . .	210
4.4	Collision algorithms and meet-in-the-middle attacks . . . . .	227
4.5	Pollard's $\rho$ method . . . . .	234
4.6	Information theory . . . . .	243
4.7	Complexity Theory and $\mathcal{P}$ versus $\mathcal{NP}$ . . . . .	258
	Exercises . . . . .	262
<b>5</b>	<b>Elliptic Curves and Cryptography</b>	<b>279</b>
5.1	Elliptic curves . . . . .	279
5.2	Elliptic curves over finite fields . . . . .	286
5.3	The elliptic curve discrete logarithm problem . . . . .	290
5.4	Elliptic curve cryptography . . . . .	296
5.5	The evolution of public key cryptography . . . . .	301
5.6	Lenstra's elliptic curve factorization algorithm . . . . .	303
5.7	Elliptic curves over $\mathbb{F}_2$ and over $\mathbb{F}_{2^k}$ . . . . .	308
5.8	Bilinear pairings on elliptic curves . . . . .	315
5.9	The Weil pairing over fields of prime power order . . . . .	325
5.10	Applications of the Weil pairing . . . . .	334
	Exercises . . . . .	339
<b>6</b>	<b>Lattices and Cryptography</b>	<b>349</b>
6.1	A congruential public key cryptosystem . . . . .	349
6.2	Subset-sum problems and knapsack cryptosystems . . . . .	352
6.3	A brief review of vector spaces . . . . .	359
6.4	Lattices: Basic definitions and properties . . . . .	363
6.5	Short vectors in lattices . . . . .	370
6.6	Babai's algorithm . . . . .	379
6.7	Cryptosystems based on hard lattice problems . . . . .	383
6.8	The GGH public key cryptosystem . . . . .	384
6.9	Convolution polynomial rings . . . . .	387
6.10	The NTRU public key cryptosystem . . . . .	392
6.11	NTRU as a lattice cryptosystem . . . . .	400
6.12	Lattice reduction algorithms . . . . .	403
6.13	Applications of LLL to cryptanalysis . . . . .	418
	Exercises . . . . .	422

---

<b>7</b>	<b>Digital Signatures</b>	<b>437</b>
7.1	What is a digital signature? . . . . .	437
7.2	RSA digital signatures . . . . .	440
7.3	ElGamal digital signatures and DSA . . . . .	442
7.4	GGH lattice-based digital signatures . . . . .	447
7.5	NTRU digital signatures . . . . .	450
	Exercises . . . . .	458
<b>8</b>	<b>Additional Topics in Cryptography</b>	<b>465</b>
8.1	Hash functions . . . . .	466
8.2	Random numbers and pseudorandom number generators . . . . .	468
8.3	Zero-knowledge proofs . . . . .	470
8.4	Secret sharing schemes . . . . .	473
8.5	Identification schemes . . . . .	474
8.6	Padding schemes and the random oracle model . . . . .	476
8.7	Building protocols from cryptographic primitives . . . . .	479
8.8	Hyperelliptic curve cryptography . . . . .	480
8.9	Quantum computing . . . . .	483
8.10	Modern symmetric cryptosystems: DES and AES . . . . .	485
	<b>List of Notation</b>	<b>489</b>
	<b>References</b>	<b>493</b>
	<b>Index</b>	<b>501</b>