

# Contents

<i>Preface</i>	<i>page</i> xv
<i>Acknowledgments</i>	xix
<hr/>	
<b>1 Introduction</b>	<b>1</b>
<hr/>	
1.1 Classical cryptography	2
1.2 Notions of cryptographic secrecy	5
1.3 Block ciphers	7
1.4 Stream ciphers	11
1.5 Public-key cryptography	13
1.6 Iterated and cascade ciphers	14
1.7 Cryptanalysis	15
1.8 Implementation attacks	18
1.9 Complexity theory	19
1.10 Authentication and identification	21
1.11 Ownership protection	23
1.12 Covert communications	24
1.13 History of information protection	25
<hr/>	
<b>2 The integers</b>	<b>32</b>
<hr/>	
2.1 Basic number theory	32
2.2 The euclidean algorithm	38
2.3 Prime fields	41
2.4 Quadratic residues	42
2.5 Quadratic reciprocity	47
2.6 The Jacobi symbol	51
2.7 Primality testing	55

<b>viii</b>	<b>Contents</b>	
	2.8 The Fermat algorithm	56
	2.9 The Solovay–Strassen algorithm	59
	2.10 The Miller–Rabin algorithm	61
	2.11 Factoring of integers	65
	2.12 The Pollard algorithm for factoring	67
	2.13 Square roots in a prime field	69
<b>3</b>	<b>Cryptography based on the integer ring</b>	82
	3.1 Biprime cryptography	83
	3.2 Implementing biprime cryptography	85
	3.3 Protocol attacks on biprime cryptography	87
	3.4 Direct attacks on biprime encryption	89
	3.5 Factoring biphimes	90
	3.6 The quadratic sieve	91
	3.7 The number-field sieve	95
	3.8 The Rabin cryptosystem	99
	3.9 The rise and fall of knapsack cryptosystems	102
<b>4</b>	<b>Cryptography based on the discrete logarithm</b>	107
	4.1 Diffie–Hellman key exchange	107
	4.2 Discrete logarithms	109
	4.3 The Elgamal cryptosystem	110
	4.4 Trapdoor one-way functions	112
	4.5 The Massey–Omura cryptosystem	113
	4.6 The Pohlig–Hellman algorithm	114
	4.7 The Shanks algorithm	121
	4.8 The Pollard algorithm for discrete logarithms	123
	4.9 The method of index calculus	127
	4.10 Complexity of the discrete-log problem	129
<b>5</b>	<b>Information-theoretic methods in cryptography</b>	135
	5.1 Probability space	136
	5.2 Entropy	137
	5.3 Perfect secrecy	139

<b>ix</b>	<b>Contents</b>	
	5.4 The Shannon–McMillan theorem	141
	5.5 Unicity distance	144
	5.6 Entropy of natural language	147
	5.7 Entropy expansion	149
	5.8 Data compaction	150
	5.9 The wiretap channel	152
<b>6</b>	<b>Block ciphers</b>	160
	6.1 Block substitution	160
	6.2 The Feistel network	162
	6.3 The Data Encryption Standard	164
	6.4 Using the Data Encryption Standard	168
	6.5 Double and triple DES encryption	170
	6.6 The Advanced Encryption Standard	171
	6.7 Differential cryptanalysis	176
	6.8 Linear cryptanalysis	177
<b>7</b>	<b>Stream ciphers</b>	181
	7.1 State-dependent encryption	182
	7.2 Additive stream ciphers	183
	7.3 Linear shift-register sequences	185
	7.4 The linear-complexity attack	189
	7.5 Analysis of linear complexity	190
	7.6 Keystreams from nonlinear feedback	194
	7.7 Keystreams from nonlinear combining	196
	7.8 Keystreams from nonlinear functions	199
	7.9 The correlation attack	207
	7.10 Pseudorandom sequences	210
	7.11 Nonlinear sets of sequences	212
<b>8</b>	<b>Authentication and ownership protection</b>	218
	8.1 Authentication	219
	8.2 Identification	219
	8.3 Authentication signatures	220

<b>x</b>	<b>Contents</b>	
	8.4 Hash functions	223
	8.5 The birthday attack	225
	8.6 Iterated hash constructions	227
	8.7 Formal hash functions	228
	8.8 Practical hash functions	230
<b>9</b>	<b>Groups, rings, and fields</b>	238
	9.1 Groups	239
	9.2 Rings	242
	9.3 Fields	243
	9.4 Prime fields	245
	9.5 Binary fields and ternary fields	246
	9.6 Univariate polynomials	247
	9.7 Extension fields	255
	9.8 The multiplication cycle in a finite field	261
	9.9 Cyclotomic polynomials	263
	9.10 Vector spaces	267
	9.11 Linear algebra	269
	9.12 The Fourier transform	272
	9.13 Existence of finite fields	276
	9.14 Bivariate polynomials	281
	9.15 Modular reduction and quotient groups	285
	9.16 Factoring of univariate polynomials	287
<b>10</b>	<b>Cryptography based on elliptic curves</b>	294
	10.1 Elliptic curves	295
	10.2 Elliptic curves over finite fields	300
	10.3 The operation of point addition	303
	10.4 The order of an elliptic curve	308
	10.5 The group of an elliptic curve	310
	10.6 Supersingular elliptic curves	312
	10.7 Elliptic curves over binary fields	315
	10.8 Computation of point multiples	319
	10.9 Elliptic curve cryptography	320
	10.10 The projective plane	323
	10.11 Point counting in an extension field	325

<b>xi</b>	<b>Contents</b>	
	10.12 Morphisms of elliptic curves over the rationals	333
	10.13 Morphisms of elliptic curves over finite fields	337
	10.14 Point counting in a ground field	343
	10.15 The method of xedni calculus	347
	10.16 Elliptic curves and the complex field	351
	10.17 Curves constructed using complex multiplication	355
<b>11</b>	<b>Cryptography based on hyperelliptic curves</b>	<b>369</b>
	11.1 Hyperelliptic curves	369
	11.2 Coordinate rings and function fields	374
	11.3 Poles and zeros	376
	11.4 Divisors	379
	11.5 Principal divisors	383
	11.6 Principal divisors on elliptic curves	385
	11.7 Jacobians as quotient groups	390
	11.8 The group of a hyperelliptic curve	392
	11.9 Semireduced divisors and jacobians	394
	11.10 The Mumford transform	396
	11.11 The Cantor reduction algorithm	402
	11.12 Reduced divisors and jacobians	405
	11.13 The Cantor–Koblitz algorithm	406
	11.14 Hyperelliptic-curve cryptography	411
	11.15 Order of the hyperelliptic jacobians	412
	11.16 Some examples of the jacobian group	414
<b>12</b>	<b>Cryptography based on bilinear pairings</b>	<b>422</b>
	12.1 Bilinear pairings	423
	12.2 Pairing-based cryptography	425
	12.3 Pairing-based key exchange	426
	12.4 Identity-based encryption	428
	12.5 Pairing-based signatures	431
	12.6 Attacks on the bilinear Diffie–Hellman protocol	432
	12.7 Torsion points and embedding degree	433
	12.8 The torsion structure theorem	438
	12.9 The structure of a pairing	446
	12.10 Attacks using bilinear pairings	448

<b>xii</b>	<b>Contents</b>	
	12.11 The Tate pairing	451
	12.12 The Miller algorithm	457
	12.13 The Weil pairing	460
	12.14 Pairing-friendly curves	464
	12.15 Barreto–Naehrig elliptic curves	465
	12.16 More pairing-friendly curves	468
<b>13</b>	<b>Implementation</b>	475
	13.1 Pairing enhancements	476
	13.2 Accelerated pairings	478
	13.3 Doubling and tripling	482
	13.4 Point representations	484
	13.5 Algorithms for elliptic-curve arithmetic	486
	13.6 Modular addition in an integer ring	487
	13.7 Modular multiplication in an integer ring	488
	13.8 Representations of binary fields	491
	13.9 Multiplication and squaring in a binary field	495
	13.10 Complementary bases	500
	13.11 Division in a finite field	503
<b>14</b>	<b>Cryptographic protocols for security and identification</b>	508
	14.1 Protocols for cryptographic security	509
	14.2 Identification protocols	510
	14.3 Zero-knowledge protocols	512
	14.4 Methods of secure identification	513
	14.5 Signature protocols	519
	14.6 Protocols for secret sharing	524
<b>15</b>	<b>More public-key cryptography</b>	527
	15.1 Introduction to lattices	528
	15.2 Elementary problems in lattice theory	535
	15.3 Reduction of a lattice basis	536
	15.4 Lattice-based cryptography	543
	15.5 Attacks on lattice cryptosystems	547

**xiii**   **Contents**

---

15.6	Introduction to codes	548
15.7	Subspace projection	552
15.8	Code-based cryptography	553
	<i>Bibliography</i>	558
	<i>Index</i>	576