
Contents

Preface	xv
I Introduction and Classical Cryptography	
1 Introduction	3
1.1 Cryptography and Modern Cryptography	3
1.2 The Setting of Private-Key Encryption	4
1.3 Historical Ciphers and Their Cryptanalysis	8
1.4 Principles of Modern Cryptography	16
1.4.1 Principle 1 – Formal Definitions	17
1.4.2 Principle 2 – Precise Assumptions	20
1.4.3 Principle 3 – Proofs of Security	22
1.4.4 Provable Security and Real-World Security	22
References and Additional Reading	23
Exercises	24
2 Perfectly Secret Encryption	25
2.1 Definitions	26
2.2 The One-Time Pad	32
2.3 Limitations of Perfect Secrecy	35
2.4 *Shannon’s Theorem	36
References and Additional Reading	37
Exercises	38
II Private-Key (Symmetric) Cryptography	
3 Private-Key Encryption	43
3.1 Computational Security	43
3.1.1 The Concrete Approach	44
3.1.2 The Asymptotic Approach	45
3.2 Defining Computationally Secure Encryption	52
3.2.1 The Basic Definition of Security	53
3.2.2 *Semantic Security	56
3.3 Constructing Secure Encryption Schemes	60
3.3.1 Pseudorandom Generators and Stream Ciphers	60
3.3.2 Proofs by Reduction	65
3.3.3 A Secure Fixed-Length Encryption Scheme	66

3.4	Stronger Security Notions	71
3.4.1	Security for Multiple Encryptions	71
3.4.2	Chosen-Plaintext Attacks and CPA-Security	73
3.5	Constructing CPA-Secure Encryption Schemes	77
3.5.1	Pseudorandom Functions and Block Ciphers	77
3.5.2	CPA-Secure Encryption from Pseudorandom Functions	82
3.6	Modes of Operation	86
3.6.1	Stream-Cipher Modes of Operation	86
3.6.2	Block-Cipher Modes of Operation	88
3.7	Chosen-Ciphertext Attacks	96
3.7.1	Defining CCA-Security	96
3.7.2	Padding-Oracle Attacks	98
	References and Additional Reading	101
	Exercises	102
4	Message Authentication Codes	107
4.1	Message Integrity	107
4.1.1	Secrecy vs. Integrity	107
4.1.2	Encryption vs. Message Authentication	108
4.2	Message Authentication Codes – Definitions	110
4.3	Constructing Secure Message Authentication Codes	116
4.3.1	A Fixed-Length MAC	116
4.3.2	Domain Extension for MACs	118
4.4	CBC-MAC	122
4.4.1	The Basic Construction	123
4.4.2	*Proof of Security	125
4.5	Authenticated Encryption	131
4.5.1	Definitions	131
4.5.2	Generic Constructions	132
4.5.3	Secure Communication Sessions	140
4.5.4	CCA-Secure Encryption	141
4.6	*Information-Theoretic MACs	142
4.6.1	Constructing Information-Theoretic MACs	143
4.6.2	Limitations on Information-Theoretic MACs	145
	References and Additional Reading	146
	Exercises	147
5	Hash Functions and Applications	153
5.1	Definitions	153
5.1.1	Collision Resistance	154
5.1.2	Weaker Notions of Security	156
5.2	Domain Extension: The Merkle–Damgård Transform	156
5.3	Message Authentication Using Hash Functions	158
5.3.1	Hash-and-MAC	159
5.3.2	HMAC	161

5.4	Generic Attacks on Hash Functions	164
5.4.1	Birthday Attacks for Finding Collisions	164
5.4.2	Small-Space Birthday Attacks	166
5.4.3	*Time/Space Tradeoffs for Inverting Functions	168
5.5	The Random-Oracle Model	174
5.5.1	The Random-Oracle Model in Detail	175
5.5.2	Is the Random-Oracle Methodology Sound?	179
5.6	Additional Applications of Hash Functions	182
5.6.1	Fingerprinting and Deduplication	182
5.6.2	Merkle Trees	183
5.6.3	Password Hashing	184
5.6.4	Key Derivation	186
5.6.5	Commitment Schemes	187
	References and Additional Reading	189
	Exercises	189
6	Practical Constructions of Symmetric-Key Primitives	193
6.1	Stream Ciphers	194
6.1.1	Linear-Feedback Shift Registers	195
6.1.2	Adding Nonlinearity	197
6.1.3	Trivium	198
6.1.4	RC4	199
6.2	Block Ciphers	202
6.2.1	Substitution-Permutation Networks	204
6.2.2	Feistel Networks	211
6.2.3	DES – The Data Encryption Standard	212
6.2.4	3DES: Increasing the Key Length of a Block Cipher	220
6.2.5	AES – The Advanced Encryption Standard	223
6.2.6	*Differential and Linear Cryptanalysis	225
6.3	Hash Functions	231
6.3.1	Hash Functions from Block Ciphers	232
6.3.2	MD5	234
6.3.3	SHA-0, SHA-1, and SHA-2	234
6.3.4	SHA-3 (Keccak)	235
	References and Additional Reading	236
	Exercises	237
7	*Theoretical Constructions of Symmetric-Key Primitives	241
7.1	One-Way Functions	242
7.1.1	Definitions	242
7.1.2	Candidate One-Way Functions	245
7.1.3	Hard-Core Predicates	246
7.2	From One-Way Functions to Pseudorandomness	248
7.3	Hard-Core Predicates from One-Way Functions	250
7.3.1	A Simple Case	250

7.3.2	A More Involved Case	251
7.3.3	The Full Proof	254
7.4	Constructing Pseudorandom Generators	257
7.4.1	Pseudorandom Generators with Minimal Expansion	258
7.4.2	Increasing the Expansion Factor	259
7.5	Constructing Pseudorandom Functions	265
7.6	Constructing (Strong) Pseudorandom Permutations	269
7.7	Assumptions for Private-Key Cryptography	273
7.8	Computational Indistinguishability	276
	References and Additional Reading	278
	Exercises	279

III Public-Key (Asymmetric) Cryptography

8	Number Theory and Cryptographic Hardness Assumptions	285
8.1	Preliminaries and Basic Group Theory	287
8.1.1	Primes and Divisibility	287
8.1.2	Modular Arithmetic	289
8.1.3	Groups	291
8.1.4	The Group \mathbb{Z}_N^*	295
8.1.5	*Isomorphisms and the Chinese Remainder Theorem	297
8.2	Primes, Factoring, and RSA	302
8.2.1	Generating Random Primes	303
8.2.2	*Primality Testing	306
8.2.3	The Factoring Assumption	311
8.2.4	The RSA Assumption	312
8.2.5	*Relating the RSA and Factoring Assumptions	314
8.3	Cryptographic Assumptions in Cyclic Groups	316
8.3.1	Cyclic Groups and Generators	316
8.3.2	The Discrete-Logarithm/Diffie–Hellman Assumptions	319
8.3.3	Working in (Subgroups of) \mathbb{Z}_p^*	322
8.3.4	Elliptic Curves	325
8.4	*Cryptographic Applications	332
8.4.1	One-Way Functions and Permutations	332
8.4.2	Constructing Collision-Resistant Hash Functions	335
	References and Additional Reading	337
	Exercises	338
9	*Algorithms for Factoring and Computing Discrete Logarithms	341
9.1	Algorithms for Factoring	342
9.1.1	Pollard’s $p - 1$ Algorithm	343
9.1.2	Pollard’s Rho Algorithm	344
9.1.3	The Quadratic Sieve Algorithm	345
9.2	Algorithms for Computing Discrete Logarithms	348

9.2.1	The Pohlig–Hellman Algorithm	350
9.2.2	The Baby-Step/Giant-Step Algorithm	352
9.2.3	Discrete Logarithms from Collisions	353
9.2.4	The Index Calculus Algorithm	354
9.3	Recommended Key Lengths	356
	References and Additional Reading	357
	Exercises	358
10	Key Management and the Public-Key Revolution	359
10.1	Key Distribution and Key Management	359
10.2	A Partial Solution: Key-Distribution Centers	361
10.3	Key Exchange and the Diffie–Hellman Protocol	363
10.4	The Public-Key Revolution	370
	References and Additional Reading	372
	Exercises	373
11	Public-Key Encryption	375
11.1	Public-Key Encryption – An Overview	375
11.2	Definitions	378
11.2.1	Security against Chosen-Plaintext Attacks	379
11.2.2	Multiple Encryptions	381
11.2.3	Security against Chosen-Ciphertext Attacks	387
11.3	Hybrid Encryption and the KEM/DEM Paradigm	389
11.3.1	CPA-Security	393
11.3.2	CCA-Security	398
11.4	CDH/DDH-Based Encryption	399
11.4.1	El Gamal Encryption	400
11.4.2	DDH-Based Key Encapsulation	404
11.4.3	*A CDH-Based KEM in the Random-Oracle Model	406
11.4.4	Chosen-Ciphertext Security and DHIES/ECIES	408
11.5	RSA Encryption	410
11.5.1	Plain RSA	410
11.5.2	Padded RSA and PKCS #1 v1.5	415
11.5.3	*CPA-Secure Encryption without Random Oracles	417
11.5.4	OAEP and RSA PKCS #1 v2.0	421
11.5.5	*A CCA-Secure KEM in the Random-Oracle Model	425
11.5.6	RSA Implementation Issues and Pitfalls	429
	References and Additional Reading	432
	Exercises	433
12	Digital Signature Schemes	439
12.1	Digital Signatures – An Overview	439
12.2	Definitions	441
12.3	The Hash-and-Sign Paradigm	443
12.4	RSA Signatures	444

12.4.1	Plain RSA	444
12.4.2	RSA-FDH and PKCS #1 v2.1	446
12.5	Signatures from the Discrete-Logarithm Problem	451
12.5.1	The Schnorr Signature Scheme	451
12.5.2	DSA and ECDSA	459
12.6	*Signatures from Hash Functions	461
12.6.1	Lamport’s Signature Scheme	461
12.6.2	Chain-Based Signatures	465
12.6.3	Tree-Based Signatures	468
12.7	*Certificates and Public-Key Infrastructures	473
12.8	Putting It All Together – SSL/TLS	479
12.9	*Signcryption	481
	References and Additional Reading	483
	Exercises	484
13	*Advanced Topics in Public-Key Encryption	487
13.1	Public-Key Encryption from Trapdoor Permutations	487
13.1.1	Trapdoor Permutations	488
13.1.2	Public-Key Encryption from Trapdoor Permutations	489
13.2	The Paillier Encryption Scheme	491
13.2.1	The Structure of $\mathbb{Z}_{N^2}^*$	492
13.2.2	The Paillier Encryption Scheme	494
13.2.3	Homomorphic Encryption	499
13.3	Secret Sharing and Threshold Encryption	501
13.3.1	Secret Sharing	501
13.3.2	Verifiable Secret Sharing	503
13.3.3	Threshold Encryption and Electronic Voting	505
13.4	The Goldwasser–Micali Encryption Scheme	507
13.4.1	Quadratic Residues Modulo a Prime	507
13.4.2	Quadratic Residues Modulo a Composite	510
13.4.3	The Quadratic Residuosity Assumption	514
13.4.4	The Goldwasser–Micali Encryption Scheme	515
13.5	The Rabin Encryption Scheme	518
13.5.1	Computing Modular Square Roots	518
13.5.2	A Trapdoor Permutation Based on Factoring	523
13.5.3	The Rabin Encryption Scheme	527
	References and Additional Reading	528
	Exercises	529
	Index of Common Notation	533

Appendix A Mathematical Background	537
A.1 Identities and Inequalities	537
A.2 Asymptotic Notation	537
A.3 Basic Probability	538
A.4 The “Birthday” Problem	542
A.5 *Finite Fields	544
Appendix B Basic Algorithmic Number Theory	547
B.1 Integer Arithmetic	549
B.1.1 Basic Operations	549
B.1.2 The Euclidean and Extended Euclidean Algorithms	550
B.2 Modular Arithmetic	552
B.2.1 Basic Operations	552
B.2.2 Computing Modular Inverses	552
B.2.3 Modular Exponentiation	553
B.2.4 *Montgomery Multiplication	556
B.2.5 Choosing a Uniform Group Element	557
B.3 *Finding a Generator of a Cyclic Group	559
B.3.1 Group-Theoretic Background	559
B.3.2 Efficient Algorithms	561
References and Additional Reading	562
Exercises	562
References	563
Index	577