

Contents

Preface	xv
1 Introduction to Cryptography	1
1.1 Cryptosystems and Basic Cryptographic Tools	1
1.1.1 Secret-key Cryptosystems	1
1.1.2 Public-key Cryptosystems	2
1.1.3 Block and Stream Ciphers	3
1.1.4 Hybrid Cryptography	3
1.2 Message Integrity	4
1.2.1 Message Authentication Codes	6
1.2.2 Signature Schemes	6
1.2.3 Nonrepudiation	7
1.2.4 Certificates	8
1.2.5 Hash Functions	8
1.3 Cryptographic Protocols	9
1.4 Security	10
1.5 Notes and References	13
2 Classical Cryptography	15
2.1 Introduction: Some Simple Cryptosystems	15
2.1.1 The Shift Cipher	17
2.1.2 The Substitution Cipher	20
2.1.3 The Affine Cipher	22
2.1.4 The Vigenère Cipher	26
2.1.5 The Hill Cipher	27
2.1.6 The Permutation Cipher	32
2.1.7 Stream Ciphers	34
2.2 Cryptanalysis	38
2.2.1 Cryptanalysis of the Affine Cipher	40
2.2.2 Cryptanalysis of the Substitution Cipher	42
2.2.3 Cryptanalysis of the Vigenère Cipher	45
2.2.4 Cryptanalysis of the Hill Cipher	48
2.2.5 Cryptanalysis of the LFSR Stream Cipher	49
2.3 Notes and References	51
Exercises	51

3	Shannon's Theory, Perfect Secrecy, and the One-Time Pad	61
3.1	Introduction	61
3.2	Elementary Probability Theory	62
3.3	Perfect Secrecy	64
3.4	Entropy	70
3.4.1	Properties of Entropy	72
3.5	Spurious Keys and Unicity Distance	75
3.6	Notes and References	79
	Exercises	80
4	Block Ciphers and Stream Ciphers	83
4.1	Introduction	83
4.2	Substitution-Permutation Networks	84
4.3	Linear Cryptanalysis	89
4.3.1	The Piling-up Lemma	89
4.3.2	Linear Approximations of S-boxes	91
4.3.3	A Linear Attack on an SPN	94
4.4	Differential Cryptanalysis	98
4.5	The Data Encryption Standard	105
4.5.1	Description of DES	105
4.5.2	Analysis of DES	107
4.6	The Advanced Encryption Standard	109
4.6.1	Description of AES	110
4.6.2	Analysis of AES	115
4.7	Modes of Operation	116
4.7.1	Padding Oracle Attack on CBC Mode	120
4.8	Stream Ciphers	122
4.8.1	Correlation Attack on a Combination Generator	123
4.8.2	Algebraic Attack on a Filter Generator	127
4.8.3	Trivium	130
4.9	Notes and References	131
	Exercises	131
5	Hash Functions and Message Authentication	137
5.1	Hash Functions and Data Integrity	137
5.2	Security of Hash Functions	139
5.2.1	The Random Oracle Model	140
5.2.2	Algorithms in the Random Oracle Model	142
5.2.3	Comparison of Security Criteria	146
5.3	Iterated Hash Functions	148
5.3.1	The Merkle-Damgård Construction	151
5.3.2	Some Examples of Iterated Hash Functions	156
5.4	The Sponge Construction	157
5.4.1	SHA-3	160
5.5	Message Authentication Codes	161

5.5.1	Nested MACs and HMAC	163
5.5.2	CBC-MAC	166
5.5.3	Authenticated Encryption	167
5.6	Unconditionally Secure MACs	170
5.6.1	Strongly Universal Hash Families	173
5.6.2	Optimality of Deception Probabilities	175
5.7	Notes and References	177
	Exercises	178
6	The RSA Cryptosystem and Factoring Integers	185
6.1	Introduction to Public-key Cryptography	185
6.2	More Number Theory	188
6.2.1	The Euclidean Algorithm	188
6.2.2	The Chinese Remainder Theorem	191
6.2.3	Other Useful Facts	194
6.3	The RSA Cryptosystem	196
6.3.1	Implementing RSA	198
6.4	Primality Testing	200
6.4.1	Legendre and Jacobi Symbols	202
6.4.2	The Solovay-Strassen Algorithm	205
6.4.3	The Miller-Rabin Algorithm	208
6.5	Square Roots Modulo n	210
6.6	Factoring Algorithms	211
6.6.1	The Pollard $p - 1$ Algorithm	212
6.6.2	The Pollard Rho Algorithm	213
6.6.3	Dixon's Random Squares Algorithm	216
6.6.4	Factoring Algorithms in Practice	221
6.7	Other Attacks on RSA	223
6.7.1	Computing $\phi(n)$	223
6.7.2	The Decryption Exponent	223
6.7.3	Wiener's Low Decryption Exponent Attack	228
6.8	The Rabin Cryptosystem	232
6.8.1	Security of the Rabin Cryptosystem	234
6.9	Semantic Security of RSA	236
6.9.1	Partial Information Concerning Plaintext Bits	237
6.9.2	Obtaining Semantic Security	239
6.10	Notes and References	245
	Exercises	246
7	Public-Key Cryptography and Discrete Logarithms	255
7.1	Introduction	255
7.1.1	The ElGamal Cryptosystem	256
7.2	Algorithms for the Discrete Logarithm Problem	258
7.2.1	Shanks' Algorithm	258
7.2.2	The Pollard Rho Discrete Logarithm Algorithm	260

7.2.3	The Pohlig-Hellman Algorithm	263
7.2.4	The Index Calculus Method	266
7.3	Lower Bounds on the Complexity of Generic Algorithms	268
7.4	Finite Fields	272
7.4.1	Joux's Index Calculus	276
7.5	Elliptic Curves	278
7.5.1	Elliptic Curves over the Reals	278
7.5.2	Elliptic Curves Modulo a Prime	281
7.5.3	Elliptic Curves over Finite Fields	284
7.5.4	Properties of Elliptic Curves	285
7.5.5	Pairings on Elliptic Curves	286
7.5.6	ElGamal Cryptosystems on Elliptic Curves	290
7.5.7	Computing Point Multiples on Elliptic Curves	292
7.6	Discrete Logarithm Algorithms in Practice	294
7.7	Security of ElGamal Systems	296
7.7.1	Bit Security of Discrete Logarithms	296
7.7.2	Semantic Security of ElGamal Systems	299
7.7.3	The Diffie-Hellman Problems	300
7.8	Notes and References	301
	Exercises	302
8	Signature Schemes	309
8.1	Introduction	309
8.1.1	RSA Signature Scheme	310
8.2	Security Requirements for Signature Schemes	312
8.2.1	Signatures and Hash Functions	313
8.3	The ElGamal Signature Scheme	314
8.3.1	Security of the ElGamal Signature Scheme	317
8.4	Variants of the ElGamal Signature Scheme	320
8.4.1	The Schnorr Signature Scheme	320
8.4.2	The Digital Signature Algorithm	322
8.4.3	The Elliptic Curve DSA	325
8.5	Full Domain Hash	326
8.6	Certificates	330
8.7	Signing and Encrypting	331
8.8	Notes and References	333
	Exercises	334
9	Post-Quantum Cryptography	341
9.1	Introduction	341
9.2	Lattice-based Cryptography	344
9.2.1	NTRU	344
9.2.2	Lattices and the Security of NTRU	348
9.2.3	Learning With Errors	351
9.3	Code-based Cryptography and the McEliece Cryptosystem	353

9.4	Multivariate Cryptography	358
9.4.1	Hidden Field Equations	359
9.4.2	The Oil and Vinegar Signature Scheme	364
9.5	Hash-based Signature Schemes	367
9.5.1	Lamport Signature Scheme	368
9.5.2	Winternitz Signature Scheme	370
9.5.3	Merkle Signature Scheme	373
9.6	Notes and References	376
	Exercises	376
10	Identification Schemes and Entity Authentication	379
10.1	Introduction	379
10.1.1	Passwords	381
10.1.2	Secure Identification Schemes	383
10.2	Challenge-and-Response in the Secret-key Setting	384
10.2.1	Attack Model and Adversarial Goals	389
10.2.2	Mutual Authentication	391
10.3	Challenge-and-Response in the Public-key Setting	394
10.3.1	Public-key Identification Schemes	394
10.4	The Schnorr Identification Scheme	397
10.4.1	Security of the Schnorr Identification Scheme	400
10.5	The Feige-Fiat-Shamir Identification Scheme	406
10.6	Notes and References	411
	Exercises	412
11	Key Distribution	415
11.1	Introduction	415
11.1.1	Attack Models and Adversarial Goals	418
11.2	Key Predistribution	419
11.2.1	Diffie-Hellman Key Predistribution	419
11.2.2	The Blom Scheme	421
11.2.3	Key Predistribution in Sensor Networks	428
11.3	Session Key Distribution Schemes	432
11.3.1	The Needham-Schroeder Scheme	432
11.3.2	The Denning-Sacco Attack on the NS Scheme	433
11.3.3	Kerberos	435
11.3.4	The Bellare-Rogaway Scheme	438
11.4	Re-keying and the Logical Key Hierarchy	441
11.5	Threshold Schemes	444
11.5.1	The Shamir Scheme	445
11.5.2	A Simplified (t, t) -threshold Scheme	448
11.5.3	Visual Threshold Schemes	450
11.6	Notes and References	454
	Exercises	454

12 Key Agreement Schemes	461
12.1 Introduction	461
12.1.1 Transport Layer Security (TLS)	461
12.2 Diffie-Hellman Key Agreement	463
12.2.1 The Station-to-station Key Agreement Scheme	465
12.2.2 Security of STS	466
12.2.3 Known Session Key Attacks	469
12.3 Key Derivation Functions	471
12.4 MTI Key Agreement Schemes	472
12.4.1 Known Session Key Attacks on MTI/A0	476
12.5 Deniable Key Agreement Schemes	478
12.6 Key Updating	481
12.7 Conference Key Agreement Schemes	484
12.8 Notes and References	488
Exercises	488
13 Miscellaneous Topics	491
13.1 Identity-based Cryptography	491
13.1.1 The Cocks Identity-based Cryptosystem	492
13.1.2 Boneh-Franklin Identity-based Cryptosystem	498
13.2 The Paillier Cryptosystem	503
13.3 Copyright Protection	506
13.3.1 Fingerprinting	507
13.3.2 Identifiable Parent Property	509
13.3.3 2-IPP Codes	511
13.3.4 Tracing Illegally Redistributed Keys	514
13.4 Bitcoin and Blockchain Technology	518
13.5 Notes and References	522
Exercises	523
A Number Theory and Algebraic Concepts for Cryptography	527
A.1 Modular Arithmetic	527
A.2 Groups	528
A.2.1 Orders of Group Elements	530
A.2.2 Cyclic Groups and Primitive Elements	531
A.2.3 Subgroups and Cosets	532
A.2.4 Group Isomorphisms and Homomorphisms	533
A.2.5 Quadratic Residues	534
A.2.6 Euclidean Algorithm	535
A.2.7 Direct Products	536
A.3 Rings	536
A.3.1 The Chinese Remainder Theorem	538
A.3.2 Ideals and Quotient Rings	539
A.4 Fields	540

B Pseudorandom Bit Generation for Cryptography	543
B.1 Bit Generators	543
B.2 Security of Pseudorandom Bit Generators	548
B.3 Notes and References	550
Bibliography	551
Index	567

The first edition of this book was published in 1993. The objective of that first was to provide a general textbook that treated all the essential concepts of cryptography as well as a selection of more advanced topics. More recently, a second edition was published in 2002 and the third edition appeared in 2008.

There have been many exciting advances in cryptography since the publication of the first edition of this book 23 years ago. At the same time, many of the “core” areas of cryptography that were important then are still relevant now—providing a strong grounding in the fundamentals remains a primary goal of this book. Many decisions had to be made in terms of which older topics to retain and which new topics should be incorporated into the book. Our choices were guided by considerations such as the relevance of practical applications of cryptography as well as the influence of new approaches and techniques to the design and analysis of cryptographic systems. In many cases, this involved studying cutting-edge research and attempting to present it in an accessible manner suitable for presentation in the classroom.

In light of the above, the basic core material of secret-key and public-key cryptography is covered in a similar fashion as in previous editions. However, there are many topics that have been added to this edition, the most important being the following:

- There is a brand new chapter on the exciting, emerging area of post-quantum cryptography, which covers the most important cryptosystems that are designed to provide security against attacks by quantum computers (Chapter 9).
- A new high-level, non-technical overview of the goals and role of cryptography has been added (Chapter 1).
- A new mathematical appendix is included, which summarizes definitions and basic results on number theory and algebra that are used throughout the book. This provides a quick way to reference any mathematical terms or formulas that a reader might wish to find (Appendix A).
- An expanded treatment of stream ciphers is provided, including common design techniques along with a description of the popular stream cipher known as ChaCha.
- The book now provides a detailed introduction to attacks on cryptosystems, including: