

Table of Contents

1	Introduction to Cryptography and Data Security	1
1.1	Overview of Cryptology (and This Book)	2
1.2	Symmetric Cryptography	5
1.2.1	Basics	5
1.2.2	Simple Symmetric Encryption: The Substitution Cipher	7
1.3	Cryptanalysis	10
1.3.1	General Thoughts on Breaking Cryptosystems	10
1.3.2	How Many Key Bits Are Enough?	13
1.4	Modular Arithmetic and More Historical Ciphers	15
1.4.1	Modular Arithmetic	15
1.4.2	Integer Rings	18
1.4.3	Shift Cipher (or Caesar Cipher)	20
1.4.4	Affine Cipher	21
1.5	Discussion and Further Reading	22
1.6	Lessons Learned	26
	Problems	28
2	Stream Ciphers	37
2.1	Introduction	38
2.1.1	Stream Ciphers vs. Block Ciphers	38
2.1.2	Encryption and Decryption with Stream Ciphers	40
2.2	Random Numbers and an Unbreakable Stream Cipher	43
2.2.1	Random Number Generators	43
2.2.2	The One-Time Pad	44
2.2.3	Towards Practical Stream Ciphers	46
2.3	Shift Register-Based Stream Ciphers	49
2.3.1	Linear Feedback Shift Registers (LFSRs)	50
2.3.2	Known-Plaintext Attack Against Single LFSRs	53
2.4	Practical Stream Ciphers	55
2.4.1	Salsa20	55
2.4.2	ChaCha	59

2.4.3	Trivium	61
2.5	Discussion and Further Reading	64
2.6	Lessons Learned	66
	Problems	68
3	The Data Encryption Standard (DES) and Alternatives	73
3.1	Introduction to DES	74
3.1.1	Confusion and Diffusion	75
3.2	Overview of the DES Algorithm	76
3.3	Internal Structure of DES	79
3.3.1	Initial and Final Permutation	80
3.3.2	The f Function	81
3.3.3	Key Schedule	86
3.4	Decryption	88
3.5	Security of DES	92
3.5.1	Exhaustive Key Search	93
3.5.2	Analytical Attacks	95
3.6	Implementation in Software and Hardware	96
3.7	DES Alternatives	97
3.7.1	The Advanced Encryption Standard (AES) and the AES Finalist Ciphers	97
3.7.2	Triple DES (3DES) and DESX	98
3.7.3	Lightweight Cipher PRESENT	99
3.8	Discussion and Further Reading	103
3.9	Lessons Learned	104
	Problems	106
4	The Advanced Encryption Standard (AES)	111
4.1	Introduction	112
4.2	Overview of the AES Algorithm	113
4.3	Some Mathematics: A Brief Introduction to Galois Fields	114
4.3.1	Existence of Finite Fields	115
4.3.2	Prime Fields	117
4.3.3	Extension Fields $GF(2^m)$	119
4.3.4	Addition and Subtraction in $GF(2^m)$	119
4.3.5	Multiplication in $GF(2^m)$	120
4.3.6	Inversion in $GF(2^m)$	122
4.4	Internal Structure of AES	124
4.4.1	Byte Substitution Layer	125
4.4.2	Diffusion Layer	128
4.4.3	Key Addition Layer	130
4.4.4	Key Schedule	130
4.5	Decryption	135
4.6	Implementation in Software and Hardware	139
4.7	Discussion and Further Reading	140

4.8	Lessons Learned	142
	Problems	143
5	More About Block Ciphers	147
5.1	Modes of Operation for Encryption and Authentication	148
5.1.1	Electronic Codebook Mode (ECB)	149
5.1.2	Cipher Block Chaining Mode (CBC) and Initialization Vectors	153
5.1.3	Output Feedback Mode (OFB)	155
5.1.4	Cipher Feedback Mode (CFB)	156
5.1.5	Counter Mode (CTR)	157
5.1.6	XTS-AES	159
5.2	Exhaustive Key Search Revisited	161
5.3	Increasing the Security of Block Ciphers	162
5.3.1	Double Encryption and Meet-in-the-Middle Attack	163
5.3.2	Triple Encryption	165
5.3.3	Key Whitening	167
5.4	Discussion and Further Reading	168
5.5	Lessons Learned	170
	Problems	171
6	Introduction to Public-Key Cryptography	177
6.1	Symmetric vs. Asymmetric Cryptography	178
6.2	Practical Aspects of Public-Key Cryptography	182
6.2.1	Security Mechanisms	183
6.2.2	The Remaining Problem: Authenticity of Public Keys	184
6.2.3	Important Public-Key Algorithms	184
6.2.4	Key Lengths and Security Levels	185
6.3	Essential Number Theory for Public-Key Algorithms	186
6.3.1	Euclidean Algorithm	187
6.3.2	Extended Euclidean Algorithm	189
6.3.3	Euler's Phi Function	195
6.3.4	Fermat's Little Theorem and Euler's Theorem	197
6.4	Discussion and Further Reading	199
6.5	Lessons Learned	200
	Problems	201
7	The RSA Cryptosystem	205
7.1	Introduction	206
7.2	Encryption and Decryption	206
7.3	Key Generation and Proof of Correctness	207
7.4	Encryption and Decryption: Fast Exponentiation	211
7.5	Speed-Up Techniques for RSA	215
7.5.1	Fast Encryption with Short Public Exponents	215
7.5.2	Fast Decryption with the Chinese Remainder Theorem	216

7.6	Finding Large Primes	219
7.6.1	How Common Are Primes?.....	220
7.6.2	Primality Tests	220
7.7	RSA in Practice: Padding	224
7.8	Key Encapsulation.....	226
7.9	Attacks	227
7.10	Implementation in Software and Hardware	231
7.11	Discussion and Further Reading	232
7.12	Lessons Learned	234
	Problems	235
8	Cryptosystems Based on the Discrete Logarithm Problem	241
8.1	Diffie–Hellman Key Exchange	242
8.2	Some Abstract Algebra.....	244
8.2.1	Groups	244
8.2.2	Cyclic Groups	246
8.2.3	Subgroups	250
8.3	The Discrete Logarithm Problem	252
8.3.1	The Discrete Logarithm Problem in Prime Fields.....	252
8.3.2	The Generalized Discrete Logarithm Problem	253
8.3.3	Attacks Against the Discrete Logarithm Problem.....	255
8.4	Security of the Diffie–Hellman Key Exchange	260
8.5	The Elgamal Encryption Scheme	261
8.5.1	From Diffie–Hellman Key Exchange to Elgamal Encryption	261
8.5.2	The Elgamal Protocol	262
8.5.3	Computational Aspects	264
8.5.4	Security	265
8.6	Discussion and Further Reading	267
8.7	Lessons Learned	268
	Problems	270
9	Elliptic Curve Cryptosystems	277
9.1	How to Compute with Elliptic Curves	278
9.1.1	Definition of Elliptic Curves	279
9.1.2	Group Operations on Elliptic Curves	281
9.2	Building a Discrete Logarithm Problem with Elliptic Curves	285
9.3	Diffie–Hellman Key Exchange with Elliptic Curves	289
9.4	Security	291
9.5	Implementation in Software and Hardware	292
9.6	Discussion and Further Reading	293
9.7	Lessons Learned	295
	Problems	296

10 Digital Signatures	299
10.1 Introduction	300
10.1.1 Odd Colors for Cars, or: Why Symmetric Cryptography Is Not Sufficient	300
10.1.2 Principles of Digital Signatures	301
10.1.3 Security Services	303
10.1.4 Applications of Digital Signatures	305
10.2 The RSA Signature Scheme	306
10.2.1 Schoolbook RSA Digital Signature	306
10.2.2 Computational Aspects	308
10.2.3 Security	309
10.3 The Elgamal Digital Signature Scheme	312
10.3.1 Schoolbook Elgamal Digital Signature	312
10.3.2 Computational Aspects	315
10.3.3 Security	315
10.4 The Digital Signature Algorithm (DSA)	318
10.4.1 The DSA Algorithm	318
10.4.2 Computational Aspects	322
10.4.3 Security	323
10.5 The Elliptic Curve Digital Signature Algorithm (ECDSA)	324
10.5.1 The ECDSA Algorithm	324
10.5.2 Computational Aspects	327
10.5.3 Security	328
10.6 Discussion and Further Reading	329
10.7 Lessons Learned	330
Problems	331
11 Hash Functions	335
11.1 Motivation: Signing Long Messages	336
11.2 Security Requirements of Hash Functions	339
11.2.1 Preimage Resistance or One-Wayness	339
11.2.2 Second Preimage Resistance or Weak Collision Resistance ..	340
11.2.3 Collision Resistance and the Birthday Attack	341
11.3 Overview of Hash Algorithms	346
11.3.1 Hash Functions from Block Ciphers	347
11.3.2 The Dedicated Hash Functions SHA-1, SHA-2 and SHA-3 ..	349
11.4 The Secure Hash Algorithm SHA-2	351
11.4.1 SHA-256 Preprocessing	352
11.4.2 The SHA-256 Compression Function	353
11.4.3 Implementation in Software and Hardware	356
11.5 The Secure Hash Algorithm SHA-3	357
11.5.1 High-Level View of SHA-3	358
11.5.2 Suffix, Padding and Output Generation	360
11.5.3 The Function Keccak- f (or the Keccak- f Permutation) ...	361
11.5.4 Other Cryptographic Functions Based on Keccak	367

11.5.5	Implementation in Software and Hardware	368
11.6	Discussion and Further Reading	369
11.7	Lessons Learned	372
	Problems	374
12	Post-Quantum Cryptography	379
12.1	Introduction	380
12.1.1	Quantum Computing and Cryptography	380
12.1.2	Quantum-Secure Asymmetric Cryptosystems	383
12.1.3	The Use of Uncertainty in Cryptography	384
12.2	Lattice-Based Cryptography	386
12.2.1	The Learning With Errors (LWE) Problem	389
12.2.2	A Simple LWE-Based Encryption System	391
12.2.3	The Ring Learning With Errors Problem	399
12.2.4	Ring-LWE Encryption Scheme	401
12.2.5	LWE in Practice	406
12.2.6	Final Remarks	408
12.3	Code-Based Cryptography	410
12.3.1	Linear Codes	411
12.3.2	The Syndrome Decoding Problem	417
12.3.3	Encryption Schemes	419
12.3.4	Suitable Choices of Codes	427
12.3.5	Final Remarks	429
12.4	Hash-Based Cryptography	430
12.4.1	One-Time Signatures	430
12.4.2	Many-Time Signatures	443
12.4.3	Final Remarks	452
12.5	PQC Standardization	453
12.6	Discussion and Further Reading	454
12.7	Lessons Learned	457
	Problems	463
13	Message Authentication Codes (MACs)	465
13.1	Principles of Message Authentication Codes	466
13.2	MACs from Hash Functions: HMAC	468
13.3	MACs from Block Ciphers	472
13.3.1	CBC-MAC	472
13.3.2	Cipher-based MAC (CMAC)	473
13.3.3	Authenticated Encryption: The Counter with Cipher Block Chaining-Message Authentication Code (CCM)	474
13.3.4	Authenticated Encryption: The Galois Counter Mode (GCM)	476
13.3.5	Galois Counter Message Authentication Code (GMAC)	478
13.4	Discussion and Further Reading	478
13.5	Lessons Learned	479
	Problems	480

14 Key Management	483
14.1 Introduction	484
14.2 Key Derivation	486
14.3 Key Establishment Using Symmetric-Key Techniques	490
14.3.1 Key Establishment with a Key Distribution Center	491
14.3.2 Needham-Schroeder Protocol	495
14.3.3 Remaining Problems with Symmetric-Key Distribution	496
14.4 Key Establishment Using Asymmetric Techniques	497
14.4.1 Man-in-the-Middle Attack	498
14.4.2 Certificates	500
14.5 Public-Key Infrastructures (PKIs) and CAs	504
14.5.1 Certificate Chains	505
14.5.2 Certificate Revocation	506
14.6 Practical Aspects of Key Management	509
14.7 Discussion and Further Reading	511
14.8 Lessons Learned	513
Problems	515
References	521
Index	535