

Table of Contents

1	Introduction to Cryptography and Data Security	1
1.1	Overview of Cryptology (and This Book)	2
1.2	Symmetric Cryptography	4
1.2.1	Basics	4
1.2.2	Simple Symmetric Encryption: The Substitution Cipher	6
1.3	Cryptanalysis	9
1.3.1	General Thoughts on Breaking Cryptosystems	9
1.3.2	How Many Key Bits Are Enough?	11
1.4	Modular Arithmetic and More Historical Ciphers	13
1.4.1	Modular Arithmetic	13
1.4.2	Integer Rings	16
1.4.3	Shift Cipher (or Caesar Cipher)	18
1.4.4	Affine Cipher	19
1.5	Discussion and Further Reading	20
1.6	Lessons Learned	22
	Problems	24
2	Stream Ciphers	29
2.1	Introduction	30
2.1.1	Stream Ciphers vs. Block Ciphers	30
2.1.2	Encryption and Decryption with Stream Ciphers	31
2.2	Random Numbers and an Unbreakable Stream Cipher	34
2.2.1	Random Number Generators	34
2.2.2	The One-Time Pad	36
2.2.3	Towards Practical Stream Ciphers	38
2.3	Shift Register-Based Stream Ciphers	41
2.3.1	Linear Feedback Shift Registers (LFSR)	41
2.3.2	Known-Plaintext Attack Against Single LFSRs	45
2.3.3	Trivium	46
2.4	Discussion and Further Reading	49
2.5	Lessons Learned	50

Problems	52
3 The Data Encryption Standard (DES) and Alternatives	55
3.1 Introduction to DES	56
3.1.1 Confusion and Diffusion	57
3.2 Overview of the DES Algorithm	58
3.3 Internal Structure of DES	61
3.3.1 Initial and Final Permutation	61
3.3.2 The f -Function	62
3.3.3 Key Schedule	67
3.4 Decryption	69
3.5 Security of DES	72
3.5.1 Exhaustive Key Search	73
3.5.2 Analytical Attacks	75
3.6 Implementation in Software and Hardware	75
3.7 DES Alternatives	77
3.7.1 The Advanced Encryption Standard (AES) and the AES Finalist Ciphers	77
3.7.2 Triple DES (3DES) and DESX	78
3.7.3 Lightweight Cipher PRESENT	78
3.8 Discussion and Further Reading	81
3.9 Lessons Learned	82
Problems	83
4 The Advanced Encryption Standard (AES)	87
4.1 Introduction	88
4.2 Overview of the AES Algorithm	89
4.3 Some Mathematics: A Brief Introduction to Galois Fields	90
4.3.1 Existence of Finite Fields	90
4.3.2 Prime Fields	93
4.3.3 Extension Fields $GF(2^m)$	94
4.3.4 Addition and Subtraction in $GF(2^m)$	95
4.3.5 Multiplication in $GF(2^m)$	96
4.3.6 Inversion in $GF(2^m)$	98
4.4 Internal Structure of AES	99
4.4.1 Byte Substitution Layer	101
4.4.2 Diffusion Layer	103
4.4.3 Key Addition Layer	106
4.4.4 Key Schedule	106
4.5 Decryption	110
4.6 Implementation in Software and Hardware	115
4.7 Discussion and Further Reading	116
4.8 Lessons Learned	117
Problems	118

5 More About Block Ciphers	123
5.1 Encryption with Block Ciphers: Modes of Operation	124
5.1.1 Electronic Codebook Mode (ECB)	124
5.1.2 Cipher Block Chaining Mode (CBC)	128
5.1.3 Output Feedback Mode (OFB)	130
5.1.4 Cipher Feedback Mode (CFB)	131
5.1.5 Counter Mode (CTR)	132
5.1.6 Galois Counter Mode (GCM)	134
5.2 Exhaustive Key Search Revisited	136
5.3 Increasing the Security of Block Ciphers	137
5.3.1 Double Encryption and Meet-in-the-Middle Attack	138
5.3.2 Triple Encryption	140
5.3.3 Key Whitening	141
5.4 Discussion and Further Reading	143
5.5 Lessons Learned	144
Problems	145
6 Introduction to Public-Key Cryptography	149
6.1 Symmetric vs. Asymmetric Cryptography	150
6.2 Practical Aspects of Public-Key Cryptography	153
6.2.1 Security Mechanisms	154
6.2.2 The Remaining Problem: Authenticity of Public Keys	154
6.2.3 Important Public-Key Algorithms	155
6.2.4 Key Lengths and Security Levels	156
6.3 Essential Number Theory for Public-Key Algorithms	157
6.3.1 Euclidean Algorithm	157
6.3.2 Extended Euclidean Algorithm	160
6.3.3 Euler's Phi Function	164
6.3.4 Fermat's Little Theorem and Euler's Theorem	166
6.4 Discussion and Further Reading	168
6.5 Lessons Learned	169
Problems	170
7 The RSA Cryptosystem	173
7.1 Introduction	174
7.2 Encryption and Decryption	174
7.3 Key Generation and Proof of Correctness	175
7.4 Encryption and Decryption: Fast Exponentiation	179
7.5 Speed-up Techniques for RSA	183
7.5.1 Fast Encryption with Short Public Exponents	183
7.5.2 Fast Decryption with the Chinese Remainder Theorem	184
7.6 Finding Large Primes	187
7.6.1 How Common Are Primes?	187
7.6.2 Primality Tests	188
7.7 RSA in Practice: Padding	192

7.8	Attacks	194
7.9	Implementation in Software and Hardware	197
7.10	Discussion and Further Reading	198
7.11	Lessons Learned	199
	Problems	200
8	Public-Key Cryptosystems Based on the Discrete Logarithm Problem	205
8.1	Diffie-Hellman Key Exchange	206
8.2	Some Algebra	208
8.2.1	Groups	208
8.2.2	Cyclic Groups	210
8.2.3	Subgroups	214
8.3	The Discrete Logarithm Problem	216
8.3.1	The Discrete Logarithm Problem in Prime Fields	216
8.3.2	The Generalized Discrete Logarithm Problem	218
8.3.3	Attacks Against the Discrete Logarithm Problem	219
8.4	Security of the Diffie-Hellman Key Exchange	225
8.5	The Elgamal Encryption Scheme	226
8.5.1	From Diffie-Hellman Key Exchange to Elgamal Encryption	226
8.5.2	The Elgamal Protocol	227
8.5.3	Computational Aspects	229
8.5.4	Security	230
8.6	Discussion and Further Reading	232
8.7	Lessons Learned	233
	Problems	234
9	Elliptic Curve Cryptosystems	239
9.1	How to Compute with Elliptic Curves	240
9.1.1	Definition of Elliptic Curves	241
9.1.2	Group Operations on Elliptic Curves	242
9.2	Building a Discrete Logarithm Problem with Elliptic Curves	246
9.3	Diffie-Hellman Key Exchange with Elliptic Curves	249
9.4	Security	251
9.5	Implementation in Software and Hardware	252
9.6	Discussion and Further Reading	253
9.7	Lessons Learned	255
	Problems	256
10	Digital Signatures	259
10.1	Introduction	260
10.1.1	Odd Colors for Cars, or: Why Symmetric Cryptography Is Not Sufficient	260
10.1.2	Principles of Digital Signatures	261
10.1.3	Security Services	263
10.2	The RSA Signature Scheme	264

10.2.1	Schoolbook RSA Digital Signature	265
10.2.2	Computational Aspects	267
10.2.3	Security	267
10.3	The Elgamal Digital Signature Scheme	270
10.3.1	Schoolbook Elgamal Digital Signature	270
10.3.2	Computational Aspects	273
10.3.3	Security	274
10.4	The Digital Signature Algorithm (DSA)	277
10.4.1	The DSA Algorithm	277
10.4.2	Computational Aspects	280
10.4.3	Security	281
10.5	The Elliptic Curve Digital Signature Algorithm (ECDSA)	282
10.5.1	The ECDSA Algorithm	282
10.5.2	Computational Aspects	285
10.5.3	Security	286
10.6	Discussion and Further Reading	287
10.7	Lessons Learned	288
	Problems	289
11	Hash Functions	293
11.1	Motivation: Signing Long Messages	294
11.2	Security Requirements of Hash Functions	296
11.2.1	Preimage Resistance or One-Wayness	297
11.2.2	Second Preimage Resistance or Weak Collision Resistance	297
11.2.3	Collision Resistance and the Birthday Attack	299
11.3	Overview of Hash Algorithms	303
11.3.1	Dedicated Hash Functions: The MD4 Family	304
11.3.2	Hash Functions from Block Ciphers	305
11.4	The Secure Hash Algorithm SHA-1	307
11.4.1	Preprocessing	308
11.4.2	Hash Computation	309
11.4.3	Implementation	312
11.5	Discussion and Further Reading	312
11.6	Lessons Learned	313
	Problems	315
12	Message Authentication Codes (MACs)	319
12.1	Principles of Message Authentication Codes	320
12.2	MACs from Hash Functions: HMAC	321
12.3	MACs from Block Ciphers: CBC-MAC	325
12.4	Galois Counter Message Authentication Code (GMAC)	326
12.5	Discussion and Further Reading	327
12.6	Lessons Learned	328
	Problems	329

13 Key Establishment	331
13.1 Introduction	332
13.1.1 Some Terminology	332
13.1.2 Key Freshness and Key Derivation	332
13.1.3 The n^2 Key Distribution Problem	334
13.2 Key Establishment Using Symmetric-Key Techniques	336
13.2.1 Key Establishment with a Key Distribution Center	336
13.2.2 Kerberos	339
13.2.3 Remaining Problems with Symmetric-Key Distribution	341
13.3 Key Establishment Using Asymmetric Techniques	342
13.3.1 Man-in-the-Middle Attack	342
13.3.2 Certificates	344
13.3.3 Public-Key Infrastructures (PKI) and CAs	347
13.4 Discussion and Further Reading	350
13.5 Lessons Learned	352
Problems	353
References	359
Index	367