

Table of Contents

1	Introduction to Cryptography and Data Security	1
1.1	Overview on the Field 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	5
1.3	Cryptanalysis	7
1.3.1	General Thoughts on Breaking Cryptosystems	7
1.3.2	How many Key Bits are Enough?	9
1.4	Modular Arithmetic and more Historical Ciphers	10
1.4.1	Modular Arithmetic	10
1.4.2	Integer Rings	12
1.4.3	Shift Cipher (or Caesar Cipher)	13
1.4.4	Affine Cipher	14
1.5	Discussion and Further Reading	16
1.6	Lessons Learned	18
	Problems	19
2	Stream Ciphers	23
2.1	Introduction	24
2.1.1	Stream Ciphers vs. Block Ciphers	24
2.1.2	Encryption and Decryption with Stream Ciphers	25
2.2	Random Numbers and an Unbreakable Stream Cipher	27
2.2.1	Random Numbers Generators	27
2.2.2	The One-Time Pad	28
2.2.3	Towards Practical Stream Ciphers	30
2.3	Shift Register-Based Stream Ciphers	32
2.3.1	Linear Feedback Shift Registers (LFSR)	32
2.3.2	Known Plaintext Attack Against Single LFSRs	35
2.3.3	Trivium	36
2.4	Discussion and Further Reading	39
2.5	Lessons Learned	40
	Problems	41
3	The Data Encryption Standard (DES) and Alternatives	43
3.1	Introduction to DES	44
3.1.1	Confusion and Diffusion	44
3.2	Overview of the DES Algorithm	45
3.3	Internal Structure of DES	48

3.3.1	Initial and Final Permutation	48
3.3.2	The f -Function	49
3.3.3	Key Schedule	53
3.4	Decryption	55
3.5	Security of DES	57
3.5.1	Exhaustive Key Search	58
3.5.2	Analytical Attacks	60
3.6	Implementation in Software and Hardware	61
3.7	DES Alternatives	61
3.7.1	The Advanced Encryption Standard and the AES Finalist Ciphers	61
3.7.2	Triple DES (3DES) and DESX	62
3.7.3	Lightweight Cipher PRESENT	62
3.8	Discussion and Further Reading	65
3.9	Lessons Learned — DES	66
	Problems	67
4	The Advanced Encryption Standard (AES)	71
4.1	Introduction	72
4.2	Overview of the AES Algorithm	72
4.3	Some Mathematics: A Brief Introduction to Galois Fields	73
4.3.1	Existence of Finite Fields	74
4.3.2	Prime Fields	75
4.3.3	Extension fields $GF(2^m)$	76
4.3.4	Addition and Subtraction in $GF(2^m)$	76
4.3.5	Multiplication in $GF(2^m)$	77
4.3.6	Inversion in $GF(2^m)$	79
4.4	Internal Structure of AES	80
4.4.1	Byte Substitution Layer	80
4.4.2	Diffusion Layer	82
4.4.3	Key Addition Layer	84
4.4.4	Key Schedule	84
4.5	Decryption	85
4.6	Implementation in Software and Hardware	87
4.7	Discussion and Further Reading	89
4.8	Lessons Learned	90
	Problems	91
5	More about Block Ciphers	101
5.1	Encryption with Block Ciphers: Modes of Operation	102
5.1.1	Electronic Codebook Mode (ECB)	102
5.1.2	Cipher Block Chaining Mode (CBC)	104
5.1.3	Output Feedback Mode (OFB)	106
5.1.4	Cipher Feedback Mode (CFB)	107
5.1.5	Counter Mode (CTR)	108
5.1.6	Galois Counter Mode (GCM)	109
5.2	Exhaustive Key Search Revisited	110
5.3	Increasing the Security of Block Ciphers	112
5.3.1	Double Encryption and Meet-in-the-Middle Attack	113
5.3.2	Triple Encryption	114
5.3.3	Key Whitening	115
5.4	Discussion and Further Reading	117
5.5	Lessons Learned	118

Problems	119
6 Introduction to Public-Key Cryptography	123
6.1 Symmetric vs. Asymmetric Cryptography	124
6.2 Practical Aspects of Public-Key Cryptography	127
6.2.1 Security Mechanisms	127
6.2.2 The Remaining Problem: Authenticity of Public Keys	127
6.2.3 Important Public-Key Algorithms	127
6.2.4 Key Lengths and Security Levels	128
6.3 Essential Number Theory for Public-Key Algorithms	129
6.3.1 Euclidean Algorithm	129
6.3.2 Extended Euclidean Algorithm	131
6.3.3 Euler's Phi Function	135
6.3.4 Fermat's Little Theorem and Euler's Theorem	136
6.4 Discussion and Further Reading	138
6.5 Lessons Learned	139
Problems	140
7 The RSA Cryptosystem	143
7.1 Introduction	144
7.2 Encryption and Decryption	144
7.3 Key Generation and Proof of Correctness	145
7.4 Encryption and Decryption: Fast Exponentiation	148
7.5 Speed-Up Techniques for RSA	150
7.5.1 Fast Encryption with Short Public Exponents	151
7.5.2 Fast Decryption with the Chinese Remainder Theorem	151
7.6 Finding Large Primes	153
7.6.1 How common are primes?	154
7.6.2 Primality Tests	154
7.7 RSA in Practice: Padding	157
7.8 Attacks	158
7.9 Implementation in Software and Hardware	160
7.10 Discussion and Further Reading	162
7.11 Lessons Learned	163
Problems	164
8 Public-Key Cryptosystems Based on the Discrete Logarithm Problem	169
8.1 Diffie-Hellman Key Exchange	170
8.2 Some Algebra	171
8.2.1 Groups	171
8.2.2 Cyclic Groups	173
8.2.3 Subgroups	175
8.3 The Discrete Logarithm Problem	177
8.3.1 The Discrete Logarithm Problem in Prime Fields	177
8.3.2 The Generalized Discrete Logarithm Problem	178
8.3.3 Attacks against the Discrete Logarithm Problem	179
8.4 Security of the Diffie-Hellman Key Exchange	183
8.5 The Elgamal Encryption Scheme	183
8.5.1 From Diffie-Hellman Key Exchange to Elgamal Encryption	184
8.5.2 The Elgamal Protocol	184
8.5.3 Computational Aspects	186
8.5.4 Security	187

8.6	Discussion and Further Reading	189
8.7	Lessons Learned	190
	Problems	191
9	Elliptic Curve Cryptosystems	195
9.1	How to Compute with Elliptic Curves	195
9.1.1	Definition of Elliptic Curves	196
9.1.2	Group Operations on Elliptic Curves	197
9.2	Building a Discrete Logarithm Problem with Elliptic Curves	200
9.3	Diffie-Hellman Key Exchange with Elliptic Curves	203
9.4	Security	205
9.5	Implementation in Software and Hardware	205
9.6	Discussion and Further Reading	207
9.7	Lessons Learned	209
	Problems	210
10	Digital Signatures	213
10.1	Introduction	214
10.1.1	Odd Colors for Cars or: Why Symmetric Cryptography is not Sufficient	214
10.1.2	Principles of Digital Signatures	215
10.1.3	Security Services	216
10.2	The RSA Signature Scheme	217
10.2.1	Schoolbook RSA Digital Signature	217
10.2.2	Computational Aspects	218
10.2.3	Security	219
10.3	The Elgamal Digital Signature Scheme	220
10.3.1	Schoolbook Elgamal Digital Signature	221
10.3.2	Computational Aspects	223
10.3.3	Security	223
10.4	The Digital Signature Algorithm (DSA)	226
10.4.1	The DSA Algorithm	226
10.4.2	Computational Aspects	228
10.4.3	Security	229
10.5	The Elliptic Curve Digital Signature Algorithm (ECDSA)	230
10.5.1	The ECDSA Algorithm	230
10.5.2	Computational Aspects	233
10.5.3	Security	233
10.6	Discussion and Further Reading	234
10.7	Lessons Learned	235
	Problems	236
11	Hash Functions	239
11.1	Motivation: Signing of Long Messages	240
11.2	Security Requirements of Hash Functions	241
11.2.1	Pre-Image Resistance or One-Wayness	242
11.2.2	Second Pre-Image Resistance or Weak Collision Resistance	243
11.2.3	Collision Resistance and the Birthday Attack	244
11.3	Overview on Hash Algorithms	247
11.3.1	Dedicated Hash Functions: The MD4-Family	247
11.3.2	Hash Functions from Block Ciphers	248
11.4	The Secure Hash Algorithm SHA-1	251
11.4.1	Preprocessing	251

11.4.2 Hash Computation	252
11.4.3 Implementation	254
11.5 Discussion and Further Reading	256
11.6 Lessons Learned	257
Problems	258
12 Message Authentication Codes (MACs)	261
12.1 Principles of Message Authentication Codes	262
12.2 MACs from Hash Functions: HMAC	264
12.3 MACs from Block Ciphers: CBC-MAC	266
12.4 GMAC	267
12.5 Discussion and Further Reading	268
12.6 Lessons Learned	269
Problems	270
13 Key Establishment	273
13.1 Introduction	274
13.1.1 Some Terminology	274
13.1.2 Key Freshness and Key Derivation	274
13.1.3 The n^2 Key Distribution Problem	276
13.2 Key Establishment Using Symmetric-Key Techniques	277
13.2.1 Key Establishment with a Key Distribution Center	277
13.2.2 Kerberos	280
13.2.3 Remaining Problems with Symmetric Key Distribution	281
13.3 Key Establishment Using Asymmetric Techniques	282
13.3.1 Man-in-the-Middle Attack	282
13.3.2 Certificates	284
13.3.3 Public-Key Infrastructures (PKI) and CAs	286
13.4 Discussion and Further Reading	290
13.5 Lessons Learned	291
Problems	292
References	295
References	295
Index	301