

Contents

Preface to <i>Cryptography Engineering</i>	xxiii	
History	xxiv	
Example Syllabi	xxiv	
Additional Information	xxvi	
Preface to <i>Practical Cryptography</i> (the 1st Edition)	xxvii	
How to Read this Book	xxix	
Part I	Introduction	1
Chapter 1	The Context of Cryptography	3
1.1	The Role of Cryptography	4
1.2	The Weakest Link Property	5
1.3	The Adversarial Setting	7
1.4	Professional Paranoia	8
1.4.1	Broader Benefits	9
1.4.2	Discussing Attacks	9
1.5	Threat Model	10
1.6	Cryptography Is Not the Solution	12
1.7	Cryptography Is Very Difficult	13
1.8	Cryptography Is the Easy Part	13
1.9	Generic Attacks	14
1.10	Security and Other Design Criteria	14
1.10.1	Security Versus Performance	14
1.10.2	Security Versus Features	17
1.10.3	Security Versus Evolving Systems	17

1.11	Further Reading	18
1.12	Exercises for Professional Paranoia	18
1.12.1	Current Event Exercises	19
1.12.2	Security Review Exercises	20
1.13	General Exercises	21
Chapter 2	Introduction to Cryptography	23
2.1	Encryption	23
2.1.1	Kerckhoffs' Principle	24
2.2	Authentication	25
2.3	Public-Key Encryption	27
2.4	Digital Signatures	29
2.5	PKI	29
2.6	Attacks	31
2.6.1	The Ciphertext-Only Model	31
2.6.2	The Known-Plaintext Model	31
2.6.3	The Chosen-Plaintext Model	32
2.6.4	The Chosen-Ciphertext Model	32
2.6.5	The Distinguishing Attack Goal	32
2.6.6	Other Types of Attack	33
2.7	Under the Hood	33
2.7.1	Birthday Attacks	33
2.7.2	Meet-in-the-Middle Attacks	34
2.8	Security Level	36
2.9	Performance	37
2.10	Complexity	37
2.11	Exercises	38
Part II	Message Security	41
Chapter 3	Block Ciphers	43
3.1	What Is a Block Cipher?	43
3.2	Types of Attack	44
3.3	The Ideal Block Cipher	46
3.4	Definition of Block Cipher Security	46
3.4.1	Parity of a Permutation	49
3.5	Real Block Ciphers	50
3.5.1	DES	51
3.5.2	AES	54
3.5.3	Serpent	56

3.5.4	Twofish	57
3.5.5	Other AES Finalists	58
3.5.6	Which Block Cipher Should I Choose?	59
3.5.7	What Key Size Should I Use?	60
3.6	Exercises	61

Chapter 4 Block Cipher Modes **63**

4.1	Padding	64
4.2	ECB	65
4.3	CBC	65
4.3.1	Fixed IV	66
4.3.2	Counter IV	66
4.3.3	Random IV	66
4.3.4	Nonce-Generated IV	67
4.4	OFB	68
4.5	CTR	70
4.6	Combined Encryption and Authentication	71
4.7	Which Mode Should I Use?	71
4.8	Information Leakage	72
4.8.1	Chances of a Collision	73
4.8.2	How to Deal With Leakage	74
4.8.3	About Our Math	75
4.9	Exercises	75

Chapter 5 Hash Functions **77**

5.1	Security of Hash Functions	78
5.2	Real Hash Functions	79
5.2.1	A Simple But Insecure Hash Function	80
5.2.2	MD5	81
5.2.3	SHA-1	82
5.2.4	SHA-224, SHA-256, SHA-384, and SHA-512	82
5.3	Weaknesses of Hash Functions	83
5.3.1	Length Extensions	83
5.3.2	Partial-Message Collision	84
5.4	Fixing the Weaknesses	84
5.4.1	Toward a Short-term Fix	85
5.4.2	A More Efficient Short-term Fix	85
5.4.3	Another Fix	87
5.5	Which Hash Function Should I Choose?	87
5.6	Exercises	87

Chapter 6	Message Authentication Codes	89
6.1	What a MAC Does	89
6.2	The Ideal MAC and MAC Security	90
6.3	CBC-MAC and CMAC	91
6.4	HMAC	93
6.5	GMAC	94
6.6	Which MAC to Choose?	95
6.7	Using a MAC	95
6.8	Exercises	97
Chapter 7	The Secure Channel	99
7.1	Properties of a Secure Channel	99
7.1.1	Roles	99
7.1.2	Key	100
7.1.3	Messages or Stream	100
7.1.4	Security Properties	101
7.2	Order of Authentication and Encryption	102
7.3	Designing a Secure Channel: Overview	104
7.3.1	Message Numbers	105
7.3.2	Authentication	106
7.3.3	Encryption	106
7.3.4	Frame Format	107
7.4	Design Details	107
7.4.1	Initialization	107
7.4.2	Sending a Message	108
7.4.3	Receiving a Message	109
7.4.4	Message Order	111
7.5	Alternatives	112
7.6	Exercises	113
Chapter 8	Implementation Issues (I)	115
8.1	Creating Correct Programs	116
8.1.1	Specifications	117
8.1.2	Test and Fix	118
8.1.3	Lax Attitude	119
8.1.4	So How Do We Proceed?	119
8.2	Creating Secure Software	120
8.3	Keeping Secrets	120
8.3.1	Wiping State	121
8.3.2	Swap File	122

8.3.3	Caches	124
8.3.4	Data Retention by Memory	125
8.3.5	Access by Others	127
8.3.6	Data Integrity	127
8.3.7	What to Do	128
8.4	Quality of Code	128
8.4.1	Simplicity	129
8.4.2	Modularization	129
8.4.3	Assertions	130
8.4.4	Buffer Overflows	131
8.4.5	Testing	131
8.5	Side-Channel Attacks	132
8.6	Beyond this Chapter	133
8.7	Exercises	133

Part III Key Negotiation 135

Chapter 9 Generating Randomness 137

9.1	Real Random	138
9.1.1	Problems With Using Real Random Data	139
9.1.2	Pseudorandom Data	140
9.1.3	Real Random Data and PRNGS	140
9.2	Attack Models for a PRNG	141
9.3	Fortuna	142
9.4	The Generator	143
9.4.1	Initialization	145
9.4.2	Reseed	145
9.4.3	Generate Blocks	146
9.4.4	Generate Random Data	146
9.4.5	Generator Speed	147
9.5	Accumulator	147
9.5.1	Entropy Sources	147
9.5.2	Pools	148
9.5.3	Implementation Considerations	150
9.5.3.1	Distribution of Events Over Pools	150
9.5.3.2	Running Time of Event Passing	151
9.5.4	Initialization	152
9.5.5	Getting Random Data	153
9.5.6	Add an Event	154
9.6	Seed File Management	155
9.6.1	Write Seed File	156

	9.6.2	Update Seed File	156
	9.6.3	When to Read and Write the Seed File	157
	9.6.4	Backups and Virtual Machines	157
	9.6.5	Atomicity of File System Updates	158
	9.6.6	First Boot	158
	9.7	Choosing Random Elements	159
	9.8	Exercises	161
Chapter 10	Primes		163
	10.1	Divisibility and Primes	163
	10.2	Generating Small Primes	166
	10.3	Computations Modulo a Prime	167
	10.3.1	Addition and Subtraction	168
	10.3.2	Multiplication	169
	10.3.3	Groups and Finite Fields	169
	10.3.4	The GCD Algorithm	170
	10.3.5	The Extended Euclidean Algorithm	171
	10.3.6	Working Modulo 2	172
	10.4	Large Primes	173
	10.4.1	Primality Testing	176
	10.4.2	Evaluating Powers	178
	10.5	Exercises	179
Chapter 11	Diffie-Hellman		181
	11.1	Groups	182
	11.2	Basic DH	183
	11.3	Man in the Middle	184
	11.4	Pitfalls	185
	11.5	Safe Primes	186
	11.6	Using a Smaller Subgroup	187
	11.7	The Size of p	188
	11.8	Practical Rules	190
	11.9	What Can Go Wrong?	191
	11.10	Exercises	193
Chapter 12	RSA		195
	12.1	Introduction	195
	12.2	The Chinese Remainder Theorem	196
	12.2.1	Garner's Formula	196
	12.2.2	Generalizations	197
	12.2.3	Uses	198
	12.2.4	Conclusion	199
	12.3	Multiplication Modulo n	199

12.4	RSA Defined	200
12.4.1	Digital Signatures with RSA	200
12.4.2	Public Exponents	201
12.4.3	The Private Key	202
12.4.4	The Size of n	203
12.4.5	Generating RSA Keys	203
12.5	Pitfalls Using RSA	205
12.6	Encryption	206
12.7	Signatures	209
12.8	Exercises	211

Chapter 13 Introduction to Cryptographic Protocols **213**

13.1	Roles	213
13.2	Trust	214
13.2.1	Risk	215
13.3	Incentive	215
13.4	Trust in Cryptographic Protocols	217
13.5	Messages and Steps	218
13.5.1	The Transport Layer	219
13.5.2	Protocol and Message Identity	219
13.5.3	Message Encoding and Parsing	220
13.5.4	Protocol Execution States	221
13.5.5	Errors	221
13.5.6	Replay and Retries	223
13.6	Exercises	225

Chapter 14 Key Negotiation **227**

14.1	The Setting	227
14.2	A First Try	228
14.3	Protocols Live Forever	229
14.4	An Authentication Convention	230
14.5	A Second Attempt	231
14.6	A Third Attempt	232
14.7	The Final Protocol	233
14.8	Different Views of the Protocol	235
14.8.1	Alice's View	235
14.8.2	Bob's View	236
14.8.3	Attacker's View	236
14.8.4	Key Compromise	238
14.9	Computational Complexity of the Protocol	238
14.9.1	Optimization Tricks	239
14.10	Protocol Complexity	240

14.11	A Gentle Warning	241
14.12	Key Negotiation from a Password	241
14.13	Exercises	241
Chapter 15	Implementation Issues (II)	243
15.1	Large Integer Arithmetic	243
15.1.1	Whooping	245
15.1.2	Checking DH Computations	248
15.1.3	Checking RSA Encryption	248
15.1.4	Checking RSA Signatures	249
15.1.5	Conclusion	249
15.2	Faster Multiplication	249
15.3	Side-Channel Attacks	250
15.3.1	Countermeasures	251
15.4	Protocols	252
15.4.1	Protocols Over a Secure Channel	253
15.4.2	Receiving a Message	253
15.4.3	Timeouts	255
15.5	Exercises	255
Part IV	Key Management	257
Chapter 16	The Clock	259
16.1	Uses for a Clock	259
16.1.1	Expiration	259
16.1.2	Unique Value	260
16.1.3	Monotonicity	260
16.1.4	Real-Time Transactions	260
16.2	Using the Real-Time Clock Chip	261
16.3	Security Dangers	262
16.3.1	Setting the Clock Back	262
16.3.2	Stopping the Clock	262
16.3.3	Setting the Clock Forward	263
16.4	Creating a Reliable Clock	264
16.5	The Same-State Problem	265
16.6	Time	266
16.7	Closing Recommendations	267
16.8	Exercises	267
Chapter 17	Key Servers	269
17.1	Basics	270
17.2	Kerberos	270

17.3	Simpler Solutions	271
	17.3.1 Secure Connection	272
	17.3.2 Setting Up a Key	272
	17.3.3 Rekeying	272
	17.3.4 Other Properties	273
17.4	What to Choose	273
17.5	Exercises	274

Chapter 18 The Dream of PKI 275

18.1	A Very Short PKI Overview	275
18.2	PKI Examples	276
	18.2.1 The Universal PKI	276
	18.2.2 VPN Access	276
	18.2.3 Electronic Banking	276
	18.2.4 Refinery Sensors	277
	18.2.5 Credit Card Organization	277
18.3	Additional Details	277
	18.3.1 Multilevel Certificates	277
	18.3.2 Expiration	278
	18.3.3 Separate Registration Authority	279
18.4	Summary	280
18.5	Exercises	280

Chapter 19 PKI Reality 281

19.1	Names	281
19.2	Authority	283
19.3	Trust	284
19.4	Indirect Authorization	285
19.5	Direct Authorization	286
19.6	Credential Systems	286
19.7	The Modified Dream	288
19.8	Revocation	289
	19.8.1 Revocation List	289
	19.8.2 Fast Expiration	290
	19.8.3 Online Certificate Verification	291
	19.8.4 Revocation Is Required	291
19.9	So What Is a PKI Good For?	292
19.10	What to Choose	293
19.11	Exercises	294

Chapter 20	PKI Practicalities	295
20.1	Certificate Format	295
20.1.1	Permission Language	295
20.1.2	The Root Key	296
20.2	The Life of a Key	297
20.3	Why Keys Wear Out	298
20.4	Going Further	300
20.5	Exercises	300
Chapter 21	Storing Secrets	301
21.1	Disk	301
21.2	Human Memory	302
21.2.1	Salting and Stretching	304
21.3	Portable Storage	306
21.4	Secure Token	306
21.5	Secure UI	307
21.6	Biometrics	308
21.7	Single Sign-On	309
21.8	Risk of Loss	310
21.9	Secret Sharing	310
21.10	Wiping Secrets	311
21.10.1	Paper	311
21.10.2	Magnetic Storage	312
21.10.3	Solid-State Storage	313
21.11	Exercises	313
Part V	Miscellaneous	315
Chapter 22	Standards and Patents	317
22.1	Standards	317
22.1.1	The Standards Process	317
22.1.1.1	The Standard	319
22.1.1.2	Functionality	319
22.1.1.3	Security	320
22.1.2	SSL	320
22.1.3	AES: Standardization by Competition	321
22.2	Patents	322
Chapter 23	Involving Experts	323
Bibliography		327
Index		339