

Practical Cryptography

Niels Ferguson

Bruce Schneier



WILEY

Wiley Publishing, Inc.

Contents

Preface	xvii
How to Read this Book	xix
1 Our Design Philosophy	1
1.1 The Evils of Performance	2
1.2 The Evils of Features	5
2 The Context of Cryptography	7
2.1 The Role of Cryptography	8
2.2 The Weakest Link Property	9
2.3 The Adversarial Setting	11
2.4 Practical Paranoia	12
2.4.1 Attack	13
2.5 Threat Model	15
2.6 Cryptography Is Not the Solution/.	17
2.7 Cryptography Is Very Difficult S.	18
2.8 Cryptography Is the Easy Part	19
2.9 Background Reading	20
3 Introduction to Cryptography	21
3.1 Encryption."	21
3.1.1 Kerckhoffs' Principle , , ••••• "	23
3.2 Authentication	23
3.3 Public-Key Encryption	26
3.4 Digital Signatures	28
3.5 PKI	29
3.6 Attacks	30

3.6.1-	Ciphertext-Only	31
3.6.2	Known Plaintext	31
3.6.3	Chosen Plaintext	32
3.6.4	Chosen Ciphertext	32
3.6.5	Distinguishing Attacks	33
3.6.6	Birthday	33
3.6.7	Meet in the Middle	34
3.6.8	Other Types of Attack	36
3.7	Security Level	36
3.8	Performance	37
3.9	Complexity	39
I	Message Security	41
4	Block Ciphers	43
4.1	What Is a Block Cipher?	43
4.2	Types of Attack	44
4.3	The Ideal Block Cipher	46
4.4	Definition of Block Cipher Security	46
4.4.1	Parity of a Permutation	49
4.5	Real Block Ciphers	50
4.5.1	DES	51
4.5.2	AES	55
4.5.3	Serpent	58
4.5.4	Twofish	59
4.5.5	Other AES Finalists	61
4.5.6	Equation-Solving Attacks	62
4.5.7	Which Block Cipher Should I Choose?	63
4.5.8	What Key Size Should I Use?	65
5	Block Cipher Modes	67
5.1	Padding	68
5.2	ECB	69
5.3	CBC	70
5.3.1	Fixed IV	70
5.3.2	Counter IV	70

5.3.3	Random IV	71
5.3.4	Nonce-Generated IV	72
5.4	OFB	73
5.5	CTR	75
5.6	Newer Modes	76
5.7	Which Mode Should I Use?	77
5.8	Information Leakage	79
5.8.1	Chances of a Collision	80
5.8.2	How to Deal With Leakage	81
5.8.3	About Our Math	82
Hash Functions		83
6.1	Security of Hash Functions	84
6.2	Real Hash Functions	86
6.2.1	MD5	87
6.2.2	SHA-1	88
6.2.3	SHA-256, SHA-384, and SHA-512	89
6.3	Weaknesses of Hash Functions	89
6.3.1	Length Extensions	90
6.3.2	Partial-Message Collision	91
6.4	Fixing the Weaknesses	92
6.4.1	A Thorough Fix	92
6.4.2	A More Efficient Fix	93
6.5	Which Hash Function Should I Choose?	95
6.6	Future Work	95
Message Authentication Codes		97
7.1	What a MAC Does	97
7.2	The Ideal MAC	98
7.3	MAC Security	98
7.4	CBC-MAC	99
7.5	HMAC	101
7.5.1	HMAC versus SHA _d	103
7.6	UMAC	104
7.6.1	Size of MAC	104
7.6.2	Which UMAC?	105
7.6.3	Platform Flexibility	106

7.6.4	Amount of Analysis	106
7.6.5	Why Mention UMAC at All? ..."	107
7.7	Which MAC to Choose?	107
7.8	Using a MAC	108
8	The Secure Channel	111
8.1	Problem Statement	
8.1.1	Roles	111
8.1.2	Key	112
8.1.3	Messages or Stream	113
8.1.4	Security Properties	113
8.2	Order of Authentication and Encryption	115
8.3	Outline	117
8.3.1	Message Numbers	117
8.3.2	Authentication	119
8.3.3	Encryption	119
8.3.4	Frame Format	120
8.4	Details	120
8.4.1	Initialization	121
8.4.2	Sending a Message	122
8.4.3	Receiving a Message	123
8.4.4	Message Order	125
8.5	Alternatives	126
8.6	Conclusion	127
9	Implementation Issues (I)	129
9.1	Creating Correct Programs	131
9.1.1	Specifications	131
9.1.2	Test and Fix	132
9.1.3	Lax ¹ Attitude	133
9.1.4	" So How Do We Proceed?"	134
9.2	Creating Secure Software	135
9.3	Keeping Secrets	136
9.3.1	Wiping State	136
9.3.2	Swap File	138
9.3.3	Caches	140
9.3.4	Data Retention by Memory	141

9.3.5	Access by Others	143
9.3.6	Data Integrity	144
9.3.7	What to Do	145
9.4	Quality of Code	146
9.4.1	Simplicity	146
9.4.2	Modularization	147
9.4.3	Assertions	148
9.4.4	Buffer Overflows	149
9.4.5	Testing	149
9.5	Side-Channel Attacks	150
9.6	Conclusion	152

II Key Negotiation 153

10 Generating Randomness 155

10.1	Real Random	156
10.1.1	Problems With Using Real Random Data	158
10.1.2	Pseudorandom Data	158
10.1.3	Real Random Data and PRNGs	159
10.2	Attack Models for a PRNG	160
10.3	Fortuna	161
10.4	The Generator	162
10.4.1	Initialization	164
10.4.2	Reseed	165
10.4.3	Generate Blocks	165
10.4.4	Generate Random Data	166
10.4.5	Generator Speed	167
10.5	Accumulator	167
10.5.1	Entropy Sources	168
10.5.2	Pools	169
10.5.3	Implementation Considerations	171
10.5.4	Initialization	174
10.5.5	Getting Random Data	174
10.5.6	Add an Event	176
10.6	Seed File Management	177
10.6.1	Write Seed File	178

10.6.2	Update Seed File	178
10.6.3	When to Read and Write the Seed File	179
10.6.4	Backups	179
10.6.5	Atomicity of File System Updates	180
10.6.6	First Boot	181
10.7	So What Should I Do?	182
10.8	Choosing Random Elements	182
11	Primes	185
11.1	Divisibility and Primes	186
11.2	Generating Small Primes	188
11.3	Computations Modulo a Prime	190
11.3.1	Addition and Subtraction	191
11.3.2	Multiplication	192
11.3.3	Groups and Finite Fields	192
11.3.4	The GCD Algorithm	194
11.3.5	The Extended Euclidean Algorithm	195
11.3.6	Working Modulo 2	197
11.4	Large Primes	197
11.4.1	Primality Testing	200
11.4.2	Evaluating Powers	204
12	Diffie-Hellman	207
12.1	Groups	208
12.2	Basic DH	210
12.3	Man in the Middle	211
12.4	Pitfalls	212
12.5	Safe Primes	214
12.6	Using a Smaller Subgroup	215
12.7	The Size of p	216
12.8	Practical Rules	218
12.9	What Could Go Wrong	220
13	RSA	223
13.1	Introduction	223
13.2	The Chinese Remainder Theorem	224
13.2.1	Garner's Formula	225

- 13.2.2 Generalizations 226
- 13.2.3 Uses 227
- 13.2.4 Conclusion 228
- 13.3 Multiplication Modulo n 228
- 13.4 RSA Defined 229
 - 13.4.1 Digital Signatures with RSA 230
 - 13.4.2 Public Exponents 230
 - 13.4.3 The Private Key 232
 - 13.4.4 The Size of n 233
 - 13.4.5 Generating RSA Keys 233
- 13.5 Pitfalls Using RSA 236
- 13.6 Encryption 237
- 13.7 Signatures 240
- 14 Introduction to Cryptographic Protocols 245**
 - 14.1 Roles 245
 - 14.2 Trust 246
 - 14.2.1 Risk 248
 - 14.3 Incentive 248
 - 14.4 Trust in Cryptographic Protocols 251
 - 14.5 Messages and Steps 251
 - 14.5.1 The Transport Layer 252
 - 14.5.2 Protocol and Message Identity 253
 - 14.5.3 Message Encoding and Parsing 254
 - 14.5.4 Protocol Execution States 255
 - 14.5.5 Errors 255
 - 14.5.6 Replay and Retries 257
- 15 Key Negotiation Protocol 261**
 - 15.1 The Setting 261
 - 15.2 A First Try 262
 - 15.3 Protocols Live Forever 264
 - 15.4 An Authentication Convention 265
 - 15.5 A Second Attempt 265
 - 15.6 A Third Attempt 267
 - 15.7 Our Final Protocol 268
 - 15.8 Different Views of the Protocol 271

15.8.1	Alice's View	271
15.8.2	Bob's View	272
15.8.3	Attacker's View	272
15.8.4	Key Compromise	273
v. 15.9	Computational Complexity of the Protocol	274
/.	15.9.1 Optimization Tricks	275
15.10	Protocol Complexity	276
15.11	A Gentle Warning	277
15.12	Key Negotiation from a Password	277
16	Implementation Issues (II)	279
16.1	Large Integer Arithmetic	279
16.1.1	Wooping	281
16.1.2	Checking DH Computations	284
16.1.3	Checking RSA Encryption	285
16.1.4	Checking RSA Signatures	286
16.1.5	Conclusion	286
16.2	Faster Multiplication	286
; .16.3	Side-Channel Attacks	288
16.3.1	Countermeasures	289
16.4	Protocols	290
16.4.1	Protocols Over a Secure Channel	291
16.4.2	-Receiving a Message	291
16.4.3	Timeouts	293
III	Key Management	295
17	The Clock	297
17.1	Uses for a Clock	297
17.1.1	Expiration	297
17.1.2	Unique Value	298
17.1.3	Monotonicity	298
17.1.4	Real-Time Transactions	299
17.2	Using the Real-Time Clock Chip	299
17.3	Security Dangers	300
17.3.1	Setting the Clock Back	> ... 300

17.3.2	Stopping the Clock	301
17.3.3	Setting the Clock Forward	302
17.4	Creating a Reliable Clock	302
17.5	The Same-State Problem	304
17.6	Time	306
• 17.7	Conclusion	307
/		
18	Key Servers	309
18.1	Basics	310
18.2	Kerberos	310
18.3	Simpler Solutions	311
18.3.1	Secure Connection	312
18.3.2	Setting Up a Key	312
18.3.3	Rekeying	313
18.3.4	Other Properties	313
18.4	What to Choose	314
/		
19	The Dream of PKI	315
19.1	A Very Short PKI Overview	315
19.2	PKI Examples	316
19.2.1	The Universal PKI	316
19.2.2	VPN Access	317
19.2.3	Electronic Banking	317
19.2.4	Refinery Sensors	317
19.2.5	Credit Card Organization /	317
19.3	Additional Details	318
19.3.1	Multilevel Certificates	318
19.3.2	Expiration	319
19.3.3	Separate Registration Authority	320
19.4	Conclusion	321
/		
20	PKI Reality	323
20.1	Names	323
20.2	Authority	326
20.3	Trust	326
20.4	Indirect Authorization	327
20.5	Direct Authorization	328

20.6	Credential Systems	• •	/	330
20.7	The Modified Dream		<i>I.</i>	332
20.8	Revocation			333
	20.8.1 Revocation List			333
	20.8.2 Fast Expiration			335
	/ 20.8.3 Revocation Is Required			335
20.9	.So What Is a PKI Good For?			336
20.10	What to Choose.			337
21	PKI Practicalities			339
21.1	Certificate Format			339
	21.1.1 • Permission Language.			340
	21.1.2 The Root Key.			340
21.2	The Life of a Key.			341
21.3	Why Keys Wear Out			343
• 21.4	So What Should You Do?			345
22	Storing Secrets			347
22.1	Disk			347
22.2	Human Memory.			348
	22.2.1 Salting and Stretching		•	350
22.3	Portable Storage.			353
22.4	Secure Token			353
22.5	Secure UI			355
22.6	Biometrics.		<i>J.</i>	356
22.7	Single Sign-On.		<	357
22.8	Risk of Loss.			358
22.9	Secret Sharing			358
22.10	Wiping Secrets.		•	360
	22.10.1 Paper.		<i>J.</i>	360
	22.10.2.-Magnetic Storage.			360
	22.10'3 Solid-State Storage.			362
IV	Miscellaneous			363
23	Standards			365
23.1	The Standards Process.			365

23.1.1	The Standard	367
23.1.2	Functionality.	367
23.1.3	Security.	368
23.2	SSL	369
23.3	AES: Standardization by Competition	370
24	Patents	373
24.1	Prior Art	373
24.2	Continuations.	374
24.3	Vagueness.	375
24.4	Reading Patents.	375
24.5	Licensing	376
24.6	Defensive Patents.	377
24.7	Fixing the Patent System.	378
24.8	Disclaimer.	379
25	Involving Experts	381
	Acknowledgments	385
/		
	Bibliography	387
	Index	397