

Contents

Preface	xix
Chapter 1 Introduction	1
Introduction	2
Threat Models	3
What Is Cryptography?	4
Cryptographic Goals	4
Privacy	4
Integrity	6
Authentication	8
Nonrepudiation	10
Goals in a Nutshell	10
Asset Management	11
Privacy and Authentication	12
Life of Data	12
Common Wisdom	13
Developer Tools	15
Summary	16
Organization	16
Frequently Asked Questions	18
Chapter 2 ASN.1 Encoding	21
Overview of ASN.1	22
ASN.1 Syntax	23
ASN.1 Explicit Values	24
ASN.1 Containers	24
ASN.1 Modifiers	26
OPTIONAL	26
DEFAULT	26
CHOICE	27
ASN.1 Data Types	28
ASN.1 Header Byte	28
Classification Bits	29
Constructed Bit	29

Primitive Types	30
ASN.1 Length Encodings	31
Short Encodings	31
Long Encodings	31
ASN.1 Boolean Type	32
ASN.1 Integer Type	33
ASN.1 BIT STRING Type	34
ASN.1 OCTET STRING Type	35
ASN.1 NULL Type	35
ASN.1 OBJECT IDENTIFIER Type	36
ASN.1 SEQUENCE and SET Types	37
SEQUENCE OF	39
SET	39
SET OF	40
ASN.1 PrintableString and IA5STRING Types	41
ASN.1 UTCTIME Type	41
Implementation	42
ASN.1 Length Routines	42
ASN.1 Primitive Encoders	45
BOOLEAN Encoding	46
INTEGER Encoding	48
BIT STRING Encoding	52
OCTET STRING Encodings	55
NULL Encoding	57
OBJECT IDENTIFIER Encodings	58
PRINTABLE and IA5 STRING Encodings	63
UTCTIME Encodings	67
SEQUENCE Encodings	71
ASN.1 Flexi Decoder	78
Putting It All Together	83
Building Lists	83
Nested Lists	85
Decoding Lists	86
FlexiLists	87
Other Providers	89
Frequently Asked Questions	90

Chapter 3 Random Number Generation	91
Introduction	92
Concept of Random	92
Measuring Entropy	94
Bit Count	95
Word Count	95
Gap Space Count	95
Autocorrelation Test	95
How Bad Can It Be?	98
RNG Design	98
RNG Events	99
Hardware Interrupts	99
Timer Skew	101
Analogue to Digital Errors	103
RNG Data Gathering	104
LFSR Basics	105
Table-based LFSRs	105
Large LFSR Implementation	107
RNG Processing and Output	107
RNG Estimation	112
Keyboard and Mouse	113
Timer	114
Generic Devices	114
RNG Setup	115
PRNG Algorithms	115
PRNG Design	115
Bit Extractors	116
Seeding and Lifetime	116
PRNG Attacks	117
Input Control	117
Malleability Attacks	118
Backtracking Attacks	118
Yarrow PRNG	118
Design	119
Reseeding	120
Statefulness	121
Pros and Cons	121
Fortuna PRNG	122

Design	122
Reseeding	126
Statefulness	126
Pros and Cons	126
NIST Hash Based DRBG	127
Design	127
Reseeding	131
Statefulness	131
Pros and Cons	131
Putting It All Together	131
RNG versus PRNG	131
Fuse Bits	132
Use of PRNGs	132
Example Platforms	133
Desktop and Server	133
Consoles	134
Network Appliances	135
Frequently Asked Questions	136
Chapter 4 Advanced Encryption Standard	139
Introduction	140
Block Ciphers	140
AES Design	142
Finite Field Math	144
AddRoundKey	146
SubBytes	146
Hardware Friendly SubBytes	149
ShiftRows	150
MixColumns	151
Last Round	155
Inverse Cipher	155
Key Schedule	155
Implementation	156
An Eight-Bit Implementation	157
Optimized Eight-Bit Implementation	162
Key Schedule Changes	165
Optimized 32-Bit Implementation	165

Precomputed Tables	165
Decryption Tables	167
Macros	168
Key Schedule	169
Performance	174
x86 Performance	174
ARM Performance	176
Performance of the Small Variant	178
Inverse Key Schedule	180
Practical Attacks	181
Side Channels	182
Processor Caches	182
Associative Caches	182
Cache Organization	183
Bernstein Attack	183
Osvik Attack	184
Defeating Side Channels	185
Little Help From the Kernel	185
Chaining Modes	186
Cipher Block Chaining	187
What's in an IV?	187
Message Lengths	188
Decryption	188
Performance Downsides	189
Implementation	189
Counter Mode	190
Message Lengths	191
Decryption	191
Performance	191
Security	191
Implementation	192
Choosing a Chaining Mode	192
Putting It All Together	193
Keying Your Cipher	193
Rekeying Your Cipher	194
Bi-Directional Channels	195
Lossy Channels	195
Myths	196

Providers	197
Frequently Asked Questions	200
Chapter 5 Hash Functions	203
Introduction	204
Hash Digests Lengths	205
Designs of SHS and Implementation	207
MD Strengthening	208
SHA-1 Design	209
SHA-1 State	209
SHA-1 Expansion	209
SHA-1 Compression	210
SHA-1 Implementation	211
SHA-256 Design	217
SHA-256 State	219
SHA-256 Expansion	219
SHA-256 Compression	219
SHA-256 Implementation	220
SHA-512 Design	225
SHA-512 State	226
SHA-512 Expansion	226
SHA-512 Compression	226
SHA-512 Implementation	226
SHA-224 Design	232
SHA-384 Design	233
Zero-Copying Hashing	234
PKCS #5 Key Derivation	236
Putting It All Together	238
What Hashes Are For	238
One-Wayness	238
Passwords	238
Random Number Generators	238
Collision Resistance	239
File Manifests	239
Intrusion Detection	239
What Hashes Are Not For	240
Unsalted Passwords	240
Hashes Make Bad Ciphers	240

Hashes Are Not MACs	240
Hashes Don't Double	241
Hashes Don't Mingle	241
Working with Passwords	242
Offline Passwords	242
Salts	242
Salt Sizes	242
Rehash	243
Online Passwords	243
Two-Factor Authentication	243
Performance Considerations	244
Inline Expansion	244
Compression Unrolling	244
Zero-Copy Hashing	245
PKCS #5 Example	245
Frequently Asked Questions	248

Chapter 6 Message-Authentication Code Algorithms 251

Introduction	252
Purpose of A MAC Function	252
Security Guidelines	253
MAC Key Lifespan	254
Standards	254
Cipher Message Authentication Code	255
Security of CMAC	257
CMAC Design	258
CMAC Initialization	259
CMAC Processing	259
CMAC Implementation	260
CMAC Performance	267
Hash Message Authentication Code	267
HMAC Design	268
HMAC Implementation	270
Putting It All Together	275
What MAC Functions Are For?	276
Consequences	276
What MAC Functions Are Not For?	278
CMAC versus HMAC	279

Replay Protection	279
Timestamps	280
Counters	280
Encrypt then MAC?	281
Encrypt then MAC	281
MAC then Encrypt	281
Encryption and Authentication	282
Frequently Asked Questions	293

Chapter 7 Encrypt and Authenticate Modes. 297

Introduction	298
Encrypt and Authenticate Modes	298
Security Goals	298
Standards	299
Design and Implementation	299
Additional Authentication Data	299
Design of GCM	300
GCM GF(2) Mathematics	300
Universal Hashing	302
GCM Definitions	302
Implementation of GCM	304
Interface	304
GCM Generic Multiplication	306
GCM Optimized Multiplication	311
GCM Initialization	312
GCM IV Processing	314
GCM AAD Processing	316
GCM Plaintext Processing	319
Terminating the GCM State	323
GCM Optimizations	324
Use of SIMD Instructions	325
Design of CCM	326
CCM B_0 Generation	327
CCM MAC Tag Generation	327
CCM Encryption	328
CCM Implementation	328
Putting It All Together	338
What Are These Modes For?	339

Choosing a Nonce	340
GCM Nonces	340
CCM Nonces	340
Additional Authentication Data	340
MAC Tag Data	341
Example Construction	341
Frequently Asked Questions	346
Chapter 8 Large Integer Arithmetic.	349
Introduction	350
What Are BigNums?	350
Further Resources	351
Key Algorithms	351
The Algorithms	351
Represent!	351
Multiplication	352
Multiplication Macros	355
Code Unrolling	359
Squaring	362
Squaring Macros	367
Montgomery Reduction	369
Montgomery Reduction Unrolling	371
Montgomery Macros	371
Putting It All Together	374
Core Algorithms	374
Size versus Speed	375
Performance BigNum Libraries	376
GNU Multiple Precision Library	376
LibTomMath Library	376
TomsFastMath Library	377
Frequently Asked Questions	378
Chapter 9 Public Key Algorithms.	379
Introduction	380
Goals of Public Key Cryptography	380
Privacy	381
Nonrepudiation and Authenticity	381
RSA Public Key Cryptography	382
RSA in a Nutshell	383

Key Generation	383
RSA Transform	384
PKCS #1	384
PKCS #1 Data Conversion	384
PKCS #1 Cryptographic Primitives	384
PKCS #1 Encryption Scheme	385
PKCS #1 Signature Scheme	386
PKCS #1 Key Format	388
RSA Security	389
RSA References	390
Elliptic Curve Cryptography	391
What Are Elliptic Curves?	392
Elliptic Curve Algebra	392
Point Addition	392
Point Doubling	393
Point Multiplication	393
Elliptic Curve Cryptosystems	394
Elliptic Curve Parameters	394
Key Generation	395
ANSI X9.63 Key Storage	395
Elliptic Curve Encryption	397
Elliptic Curve Signatures	398
Elliptic Curve Performance	400
Jacobian Projective Points	400
Point Multiplication Algorithms	401
Putting It All Together	402
ECC versus RSA	402
Speed	402
Size	404
Security	404
Standards	404
References	405
Text References	405
Source Code References	405
Frequently Asked Questions	406
Index.....	409