

Contents

1	History of Cryptography to the 1800s.	1
	Introduction.	1
	In This Chapter We Will Cover the Following	2
	Why Study Cryptography?	2
	What Is Cryptography?	3
	Substitution Ciphers	5
	The Caesar Cipher.	5
	Atbash Cipher	8
	Affine Ciphers.	9
	Homophonic Substitution	11
	Polybius Cipher.	12
	Null Cipher	13
	Multi-alphabet Substitution	14
	Devices	17
	Phaistos Disc.	19
	Phryctoriae	20
	Book Ciphers	20
	Transposition Ciphers	21
	Reverse Order	21
	Rail Fence Cipher	22
	Geometric Shape Cipher.	22
	Columnar Cipher.	23
	Combinations	24
	D'Agapeyeff Cipher	25
	Conclusions.	26
	Test Your Knowledge	26
	References.	27
2	History of Cryptography from the 1800s	29
	Introduction.	29
	In This Chapter We Will Cover the Following	29

Playfair	30
Two-Square Cipher	31
Four-Square Cipher	33
Hill Cipher	35
ADFGVX	36
Bifid	38
The Gronsfeld Cipher	39
The Vernam Cipher	40
Edgar Allan Poe	40
Cryptography Comes of Age	41
Enigma	41
Kryha	43
SIGABA	44
Lorenz Cipher	45
Navajo Code Talkers	45
VIC Cipher	46
IFF Systems	46
The NSA: The Early Years	47
Conclusions	48
Test Your Knowledge	49
References	49
3 Basic Information Theory	51
Introduction	51
In This Chapter We Will Cover	51
The Information Age	52
Claude Shannon	53
Theorem 1: Shannon's Source Coding Theorem	55
Theorem 2: Noisy Channel Theorem	55
Concepts	55
Information Entropy	56
Quantifying Information	58
Confusion and Diffusion	59
Avalanche	60
Hamming Distance	61
Hamming Weight	61
Kerckhoffs's Principle/Shannon's Maxim	62
Information Diversity	63
Scientific and Mathematical Theories	64
What Is a Mathematical Theory?	65
The Scientific Process	66
A Scientific Theory	66
Binary Math	69
Converting	70
Binary Operations	70

Conclusions.....	72
Test Your Knowledge	72
References.....	73
4 Essential Number Theory and Discrete Math	75
Introduction.....	75
In This Chapter We Will Cover.....	76
Number Systems.....	76
Natural Numbers.....	77
Integers	77
Rational Numbers	78
Irrational Numbers	78
Real Numbers	78
Complex Numbers	79
Transcendental Numbers.....	82
Prime Numbers	83
Finding Prime Numbers	83
Relatively Prime	88
Important Operations	89
Divisibility Theorems	90
Summation	90
Logarithms	91
Modulus Operations	92
Famous Number Theorists and Their Contributions.....	94
Fibonacci.....	94
Fermat.....	95
Euler	95
Goldbach.....	96
Discrete Mathematics	96
Set Theory.....	97
Logic.....	99
Combinatorics.....	104
Conclusions.....	106
Test Your Knowledge	107
References.....	107
5 Essential Algebra.....	109
Introduction.....	109
In This Chapter We Will Cover.....	110
Groups, Rings, and Fields.....	110
Groups.....	112
Rings.....	113
Fields.....	114
Diophantine Equations	115
Linear Algebra	116
Matrix Addition and Multiplication	117

Matrix Transposition	120
Submatrix	121
Identity Matrix	122
Determinants	123
Eigenvalues and Eigenvectors	125
Vector Spaces	129
Algorithms	131
Basic Algorithms	131
Sorting Algorithms	132
Conclusions	137
Test Your Knowledge	137
References	138
6 Feistel Networks	139
Introduction	139
Cryptographic Keys	141
Feistel Function	142
Unbalanced Feistel	144
Pseudo-Hadamard Transform	144
MDS Matrix	145
Lucifer	145
DES	147
3DES	150
s-box and p-box	151
DEAL	152
MacGuffin	152
GOST	152
Blowfish	153
Twofish	154
Skipjack	156
CAST	158
FEAL	159
MARS	159
TEA	160
XTEA	161
LOKI97	162
Camellia	162
ICE	162
Simon	163
IDEA	163
MISTY1	163
KASUMI	163
MAGENTA	164
Speck	164
Symmetric Methods	165

ECB	165
CBC	165
PCBC	166
CFB	166
Galois/Counter Mode	167
Conclusions	167
Test Your Knowledge	167
References	168
7 Substitution-Permutation Networks	169
Introduction	169
In This Chapter We Will Cover	169
Replacing DES	169
AES	170
Rijndael Steps	171
Rijndael Outline	172
Rijndael s-box	173
Rijndael Key Schedule	174
Serpent	176
Serpent s-boxes	176
Serpent Key Schedule	178
The Serpent Algorithm	178
Square	178
SHARK	179
SAFER	179
The Round Function	180
Key Schedule	180
KHAZAD	182
NESSIE	182
Stream Ciphers	183
LFSR	184
RC4	184
FISH	186
eSTREAM	187
Salsa20	189
One-Time Pad	189
Conclusions	190
Test Your Knowledge	190
References	191
8 s-box Design	193
Introduction	193
Why Study s-box Design?	193
Critical to Block Ciphers	194
Designing Ciphers	194
Altering s-boxes	195

General Facts About s-boxes	195
Types of s-boxes	196
Design Considerations	197
Approaches to s-box Design	199
DES s-box	200
The Actual s-boxes for DES	200
The Rijndael s-box	202
The Irreducible Polynomial	203
Multiplicative Inverse	204
Affine Transformation	206
Generating the s-box	206
Changing the Rijndael s-box	207
s-box Variations	208
Key-Dependent s-boxes	208
Chaos-Driven s-boxes	210
Conclusions	211
Test Your Knowledge	211
References	212
9 Cryptographic Hashes	213
Introduction	213
In This Chapter We Will Cover	213
What Is a Cryptographic Hash?	214
How Are Cryptographic Hashes Used?	215
Message Integrity	215
Password Storage	216
Forensic Integrity	217
Merkle-Damgard	218
Specific Algorithms	218
Checksums	219
MD5	220
SHA	221
RIPEMD	225
Tiger	226
HAVAL	226
NTLM	226
Whirlpool	227
Skein	227
FSB	228
GOST	228
BLAKE	229
Grøstl	229
SWIFFT	229
MAC and HMAC	229

Key Derivation Functions	230
Conclusions.	230
Test Your Knowledge	231
References.	231
10 Asymmetric Algorithms	233
Introduction.	233
In This Chapter We Will Cover the Following	233
What Is Asymmetric Cryptography?	233
Indistinguishability	234
RSA.	235
RSA Example 1.	237
RSA Example 2.	237
Factoring RSA Keys	238
The Rabin Cryptosystem.	239
Diffie–Hellman	239
ElGamal	240
MQV	241
YAK	242
Forward Secrecy	242
Optimal Asymmetric Encryption Padding	243
Cramer–Shoup	243
Applications	243
Key Exchange	244
Digital Signatures	244
Digital Certificates	246
SSL/TLS	249
Homomorphic Encryption	251
Conclusions.	251
Test Your Knowledge	251
References.	252
11 Elliptic Curve Cryptography	253
Introduction.	253
In This Chapter, We Will Cover the Following	253
General Overview	254
Basic Operations on Elliptic Curves	255
The Algorithm.	258
ECC Variations	260
ECC Diffie–Hellman	261
ECC DSA	261
Conclusions.	262
Test Your Knowledge	263
References.	263

12 Random Number Generators	265
Introduction	265
In This Chapter We Will Cover	266
What Makes a Good PRNG?	266
Desirable Properties of Pseudorandom Numbers	266
Tests of Randomness	267
Standards for PRNG	272
Specific Algorithms	272
Mid-Square	272
Linear Congruential Generator	273
Mersenne Twister	277
Blum Blum Shub	279
Yarrow	280
Fortuna	281
DUAL_EC_DRBG	281
The Marsaglia CD ROM	282
Improving PRNGs	283
Shuffling	283
Cryptographic Hash	283
Conclusions	283
Test Your Knowledge	284
References	284
13 SSL/TLS	285
Introduction	285
In This Chapter We Will Cover	285
Digital Signatures	286
Direct Signature	286
Arbitrated Digital Signature	287
Digital Certificates	288
X.509	289
PGP	293
Alternate Certificate Types	293
Public Key Infrastructure X.509	294
SSL and TLS	295
History	296
The Handshake Step by Step	297
Applications of SSL/TLS	300
Conclusions	307
Test Your Knowledge	307
References	307
14 Virtual Private Networks, Authentication, and Wireless Security ..	309
Introduction	309
In This Chapter We Will Cover	309
Concepts	310

Authentication	310
CHAP	312
EAP	313
Kerberos	314
SESAME	316
NTLM	316
PPTP	317
PPTP Authentication	318
PPTP Encryption	318
L2TP	319
IPSec	319
IKE Phase 1	321
IKE Phase 2	322
VPN Gateways and Concentrators	322
SSL/TLS	323
Other Secure Communications	323
SSH	323
Wi-Fi Encryption	325
Conclusions	327
Test Your Knowledge	327
References	327
15 Military Applications	329
Introduction	329
In This Chapter We Will Cover	330
NSA and Cryptography	330
Security Classifications	330
NSA Cryptographic Standards	331
FIREFLY	335
The Modern Role of the NSA	335
Secure Phones	336
US Cryptography Laws and Regulations	336
How Do Other Nations Handle Cryptography?	337
International Regulations and Agreements	337
Cryptography and Malware	340
Weaponized Malware	341
Cyber Warfare	342
TOR	343
TOR Technical Details	345
Conclusions	346
Test Your Knowledge	346
References	347
16 Steganography	349
Introduction	349
In This Chapter We Will Cover	349

What Is Steganography?	349
Historical Steganography	352
Methods and Tools	353
Classes of Steganography	354
Tools	356
Current Use of Steganography	362
Steganalysis.	364
Distributed Steganography	365
Total Blocks and Block Order.	366
Conclusions.	368
Test Your Knowledge	369
References.	369
17 Cryptanalysis.	371
Introduction.	371
In This Chapter We Will Cover.	372
Classic Methods	372
Frequency Analysis.	372
Kasiski.	373
Modern Methods.	373
Linear Cryptanalysis.	374
Differential Cryptanalysis.	375
Integral Cryptanalysis.	377
Mod-n Cryptanalysis.	377
Asymmetric Cryptanalysis	378
General Rules for Cryptanalysis.	379
Rainbow Tables.	380
The Birthday Paradox	382
Other Methods	383
Other Passwords	383
Related Data	384
Spyware.	384
Resources	384
Conclusions.	384
Test Your Knowledge	385
References.	385
18 Cryptographic Backdoors	387
Introduction.	387
In This Chapter We Will Cover.	387
What Are Cryptographic Backdoors?	388
General Concepts	388
Output Indistinguishability	388
Confidentiality.	389
Ability to Compromise the Backdoor.	389
Specific Examples.	390

	Dual_EC_DRBG	390
	Details	390
	RSA Backdoor	391
	Compromising a Hashing Algorithm	392
	The Prevalence of Backdoors	393
	Governmental Approach	393
	Private Citizen/Group Approach	394
	Countermeasures	394
	Conclusions	395
	Test Your Knowledge	396
	References	396
19	Quantum Computing and Cryptography	397
	Introduction	397
	What This Means for Cryptography	398
	What Is a Quantum Computer?	399
	Quantum Physics Basics	401
	Physical Qubits	404
	Possible Quantum-Resistant Cryptographic Algorithms	405
	Conclusions	406
	Test Your Knowledge	406
	References	407
20	Lattice-Based Cryptography	409
	Introduction	409
	Lattice-Based Mathematical Problems	410
	Shortest Integer Problem	412
	Closest Vector Problem	413
	Cryptographic Algorithms	414
	NTRU	414
	GGH	417
	Peikert's Ring	419
	Solving Lattice Problems	421
	Lenstra-Lenstra-Lovász (LLL)	422
	Conclusions	424
	Test Your Knowledge	424
	References	425
21	More Approaches to Quantum-Resistant Cryptography	427
	Introduction	427
	Multivariate Cryptography	427
	Mathematics	427
	Matsumoto-Imai	429
	Hidden Field Equations	431
	Multivariate Quadratic Digital Signature (MQDSS)	433
	SFLASH	434

SWIFFT	435
Lamport Signature	438
Code-Based Cryptography	438
McEliece	439
Niederreiter Cryptosystem	441
Supersingular Isogeny Key Exchange	441
Elliptic Curves	442
SIDH	444
Conclusions.	448
Test Your Knowledge	448
References.	449
Index.	451