

Contents

1	History of Cryptography to the 1800s	1
	Introduction	1
	In This Chapter We Will Cover	2
	Why Study Cryptography?	2
	What Is Cryptography?	3
	Substitution Ciphers	5
	The Caesar Cipher	5
	Atbash Cipher	8
	Affine Ciphers	9
	Homophonic Substitution	10
	Polybius Cipher	12
	Null Cipher	13
	Multi-Alphabet Substitution	13
	Devices	17
	Book Ciphers	19
	Transposition Ciphers	20
	Reverse Order	20
	Rail Fence Cipher	21
	Geometric Shape Cipher	21
	Columnar Cipher	22
	Combinations	23
	D'Agapeyeff Cipher	24
	Conclusions	24
	Test Your Knowledge	25
	References	26
2	History of Cryptography from the 1800s	27
	Introduction	27
	In This Chapter We Will Cover	28
	Playfair	28
	Two-Square Cipher	30

Four-Square Cipher	33
Hill Cipher	34
ADFGVX	36
Bifid	38
The Gronsfeld Cipher	39
The Vernam Cipher	39
Edgar Allen Poe	40
Cryptography Comes of Age	41
Enigma	41
SIGABA	43
Lorenz Cipher	44
Navajo Code Talkers	45
VIC Cipher	45
IFF Systems	46
The NSA—The Early Years	47
Conclusions	48
Test Your Knowledge	48
References	49
3 Basic Information Theory	51
Introduction	51
In This Chapter We Will Cover	52
The Information Age	52
Claude Shannon	54
Theorem 1: Shannon's Source Coding Theorem	55
Theorem 2: Noisy Channel Theorem	55
Concepts	56
Information Entropy	56
Quantifying Information	58
Confusion & Diffusion	59
Avalanche	61
Hamming Distance	61
Hamming Weight	61
Kerckhoffs's Principle/Shannon's Maxim	62
Scientific and Mathematical Theories	63
What Is a Mathematical Theory?	64
The Scientific Process	65
A Scientific Theory	65
Binary Math	68
Converting	69
Binary Operations	69
Conclusions	71
Test Your Knowledge	72
References	72

4	Essential Number Theory and Discrete Math	73
	Introduction	73
	In This Chapter We Will Cover	74
	Number Systems	74
	Natural Numbers	75
	Integers	75
	Rational Numbers	75
	Irrational Numbers	76
	Real Numbers	76
	Complex Numbers	76
	Transcendental Numbers	77
	Prime Numbers	78
	Finding Prime Numbers	79
	Relatively Prime	84
	Important Operations	85
	Divisibility Theorems	86
	Summation	86
	Logarithms	87
	Modulus Operations	88
	Famous Number Theorists and Their Contributions	90
	Fibonacci	90
	Fermat	91
	Euler	92
	Goldbach	92
	Discrete Mathematics	93
	Set Theory	93
	Logic	95
	Combinatorics	100
	Conclusions	103
	Test Your Knowledge	103
	References	104
5	Essential Algebra	105
	Introduction	105
	In This Chapter We Will Cover	106
	Groups, Rings, and Fields	106
	Groups	108
	Rings	109
	Fields	110
	Diophantine Equations	111
	Linear Algebra	112
	Matrix Addition and Multiplication	113
	Matrix Transposition	116
	Submatrix	117
	Identity Matrix	118

Determinants	119
Eigenvalues and Eigenvectors	121
Algorithms	124
Basic Algorithms	124
Sorting Algorithms	126
Conclusions	131
Test Your Knowledge	131
References	132
6 Feistel Networks	133
Introduction	133
Cryptographic Keys	135
Feistel Function	135
Unbalanced Feistel	138
Pseudo-Hadamard Transform	138
MDS Matrix	139
Lucifer	139
DES	141
3DES	144
S-Box and P-Box	146
DEAL	146
McGuffin	146
GOST	147
Blowfish	147
Twofish	149
Skipjack	151
CAST	153
FEAL	153
MARS	153
TEA	154
XTEA	156
LOKI97	156
Camellia	157
ICE	157
Simon	157
IDEA	157
MISTY1	158
KASUMI	158
MAGENTA	158
Speck	159
Symmetric Methods	159
ECB	160
CBC	160
PCBC	161
CFB	161
Galois/Counter Mode	161

Conclusions	162
Test Your Knowledge	162
References	163
7 Substitution–Permutation Networks	165
Introduction	165
In This Chapter We Will Cover	165
Replacing DES	166
AES	166
Rijndael Steps	167
Rijndael Outline	168
Rijndael S-Box	169
Rijndael Key Schedule	170
Serpent	172
Serpent S-Boxes	172
Serpent Key Schedule	173
The Serpent Algorithm	173
Square	174
SHARK	174
SAFER	175
The Round Function	176
Key Schedule	176
KHAZAD	176
NESSIE	177
Stream Ciphers	178
LFSR	179
RC4	179
FISH	181
eSTREAM	182
Salsa20	184
One-Time Pad	184
Conclusions	185
Test Your Knowledge	185
References	186
8 S-Box Design	187
Introduction	187
Why Study S-Box Design?	187
Critical to Block Ciphers	188
Designing Ciphers	188
Altering S-Boxes	189
General Facts about S-Boxes	189
Types of S-Boxes	190
Design Considerations	192
Approaches to S-Box Design	194

DES S-Box	194
The Actual S-Boxes for DES	194
The Rijndael S-Box	196
The Irreducible Polynomial	197
Multiplicative Inverse	198
Affine Transformation	199
Generating the S-Box	200
Changing the Rijndael S-Box	202
Conclusions	203
Test Your Knowledge	203
References	204
9 Cryptographic Hashes	205
Introduction	205
In This Chapter, We Will Cover	206
What Is a Cryptographic Hash?	206
How Are Cryptographic Hashes Used?	207
Message Integrity	207
Password Storage	208
Forensic Integrity	209
Merkle-Damgard	210
Specific Algorithms	211
Checksums	211
MD5	212
SHA	214
RipeMD	217
Tiger	218
HAVAL	218
NTLM	219
Whirlpool	220
Skein	220
FSB	220
Gost	221
BLAKE	221
Grøstl	221
SWIFFT	221
MAC and HMAC	222
Key Derivation Functions	222
Conclusions	223
Test Your Knowledge	223
References	224
10 Asymmetric Algorithms	225
Introduction	225
In This Chapter, We Will Cover	225

What Is Asymmetric Cryptography?	226
RSA	227
RSA Example 1	229
RSA Example 2	229
Factoring RSA Keys	230
The Rabin Cryptosystem	231
Diffie–Hellman	231
ElGamal	232
MQV	233
YAK	234
Forward Secrecy	235
Optimal Asymmetric Encryption Padding	235
Cramer–Shoup	235
Applications	236
Key Exchange	236
Digital Signatures	236
Digital Certificates	239
SSL/TLS	241
Homomorphic Encryption	243
Conclusions	243
Test Your Knowledge	244
References	244
11 Elliptic Curve Cryptography	245
Introduction	245
In This Chapter, We Will Cover	246
General Overview	246
Basic Operations on Elliptic Curves	248
The Algorithm	251
ECC Variations	253
ECC Diffie–Hellman	253
ECC DSA	254
Conclusions	255
Test Your Knowledge	255
References	256
12 Random Number Generators	257
Introduction	257
In This Chapter, We Will Cover	258
What Makes a Good PRNG?	258
Desirable Properties of Pseudorandom Numbers	258
Tests of Randomness	259
Standards for PRNG	264
Specific Algorithms	265
Mid-Square	265
Linear Congruential Generator	266

	Mersenne Twister	270
	Blum–Blum–Shub	271
	Yarrow	271
	Fortuna	273
	DUAL_EC_DRBG	273
	The Marsaglia CD ROM	274
	Improving PRNGs	274
	Shuffling	275
	Cryptographic Hash	275
	Conclusions	275
	Test Your Knowledge	276
	References	276
13	SSL/TLS	277
	Introduction	277
	In This Chapter We Will Cover	277
	Digital Signatures	278
	Direct Signature	278
	Arbitrated Digital Signature	279
	Digital Certificates	280
	X.509	281
	PGP	283
	Public Key Infrastructure X.509	284
	SSL and TLS	285
	History	286
	The Handshake Step By Step	287
	Applications of SSL/TLS	290
	Conclusions	296
	Test Your Knowledge	297
	References	298
14	Virtual Private Networks, Authentication, and Wireless Security	299
	Introduction	299
	In This Chapter We Will Cover	299
	Concepts	300
	Authentication	300
	CHAP	302
	EAP	302
	Kerberos	304
	SESAME	306
	NTLM	306
	PPTP	307
	PPTP Authentication	308
	PPTP Encryption	308
	L2TP	308

- IPSEC 309
 - IKE Phase 1 310
 - IKE Phase 2 311
- SSL/TLS 312
- Other Secure Communications 313
 - SSH 313
 - Wi-Fi Encryption 314
- Conclusions 316
- Test Your Knowledge 316
- References 317

- 15 Military Applications 319**
 - Introduction 319
 - In This Chapter We Will Cover 320
 - NSA and Cryptography 320
 - Security Classifications 320
 - NSA Cryptographic Standards 321
 - The Modern Role of the NSA 325
 - U.S. Cryptography Laws and Regulations 325
 - How Do Other Nations Handle Cryptography? 326
 - International Regulations and Agreements 327
 - Cryptography and Malware 329
 - Weaponized Malware 330
 - Cyber Warfare 331
 - TOR 333
 - Conclusions 335
 - Test Your Knowledge 335
 - References 335

- 16 Steganography 337**
 - Introduction 337
 - In This Chapter We Cover 337
 - What Is Steganography? 337
 - Historical Steganography 340
 - Methods and Tools 341
 - Classes of Steganography 342
 - Tools 344
 - Current Use of Steganography 351
 - Steganalysis 351
 - Distributed Steganography 353
 - Total Blocks and Block Order 353
 - Conclusions 355
 - Test Your Knowledge 356
 - References 356

17	Cryptanalysis	357
	Introduction	357
	In This Chapter We Will Cover	358
	Classic Methods	358
	Frequency Analysis	358
	Kasiski	359
	Modern Methods	360
	Linear Cryptanalysis	360
	Differential Cryptanalysis	361
	Integral Cryptanalysis	363
	Mod-n Cryptanalysis	363
	Asymmetric Cryptanalysis	364
	General Rules for Cryptanalysis	366
	Rainbow Tables	366
	The Birthday Paradox	367
	Other Methods	369
	Other Passwords	369
	Related Data	370
	Spyware	370
	Resources	371
	Conclusions	371
	Test Your Knowledge	371
	References	372
18	Cryptographic Backdoors	373
	Introduction	373
	In This Chapter We Will Cover	374
	What Are Cryptographic Backdoors?	374
	General Concepts	375
	Output Indistinguishability	375
	Confidentiality	375
	Ability to Compromise the Backdoor	375
	Specific Examples	376
	Dual_EC_DRBG	376
	Details	377
	RSA Backdoor	378
	Compromising a Hashing Algorithm	379
	The Prevalence of Backdoors	379
	Governmental Approach	379
	Private Citizen/Group Approach	380
	Counter Measures	381
	Conclusions	382
	Test Your Knowledge	382
	References	383

19 Quantum Computing and Cryptography 385

 Introduction 385

 What This Means for Cryptography 386

 What Is a Quantum Computer? 387

 Possible Quantum Resistant Cryptographic Algorithms 388

 Conclusions 390

 Test Your Knowledge 390

 References 390

Introduction

Cryptography is an important but difficult topic. A great many professions require some level of use of cryptography. This includes programmers, network administrators, and cybersecurity professionals. However, such people often are not provided adequate training in cryptography. There are a number of excellent cryptography books available, but most assume some level of mathematical sophistication on the part of the reader. This renders them inaccessible to a substantial number of potential readers.

The entire purpose of this book is to bridge this gap. If you are a mathematician or cryptographer, this book is not intended for you. In fact, you might feel frustrated that certain mathematical details are not fully explored. As one glaring example, there are no mathematical proofs in this book. This book is aimed at the person who wants or needs a better understanding of cryptography, but may not have a background in number theory, linear algebra, and other similar topics. When needed, just enough math is provided for you to follow along, and no more detail than is necessary. As a consequence, this book is meant to be accessible to a broad audience. However, that also means that should you master every topic in this book, you would not be a cryptographer. You will, however, be an intelligent consumer of cryptography. You will know the questions to ask vendors, and be able to understand and evaluate their responses.

There are a great many practical questions this book will prepare you to analyze. Should you use elliptic curve or RSA? If you wish to use RSA, what is the appropriate key size? What makes a good cryptographic hashing algorithm? Why is an HMAC better than a hash? Why should you always use CBC mode with symmetric ciphers? What impact will quantum computing have on the current cryptography? These are just a few of the questions you will gain answers to in this book.

Furthermore, this book should provide you a solid foundation should you later wish to delve into more mathematically rigorous cryptography books. Having

studied this book, you will be able to venture into deeper waters. There are some excellent books from Springer that go deeper into the mathematics. *Understanding Cryptography* by Paar and Pelsl is one such book. For readers who really want to dive into the math, *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman is an excellent choice.