

Contents

Preface	vii
Introduction	1
Basic Concepts	4
The Caesar Cipher	7
The Affine Cipher	8
The One-Time Pad	11
Kerckhoffs' Principle	15
Part I. Data Encryption	19
1 Monoalphabetic Substitution Ciphers	21
1.1 Letter Distributions	22
1.2 Breaking a Monoalphabetic Cipher	24
1.3 The Pigpen Cipher	28
1.4 Polybius's Monoalphabetic Cipher	29
1.5 Extended Monoalphabetic Ciphers	30
1.6 The Playfair Cipher	30
1.7 Homophonic Substitution Ciphers	35
2 Transposition Ciphers	39
2.1 Simple Examples	40
2.2 Cyclic Notation and Keys	44
2.3 Transposition by Turning Template	45
2.4 Columnar Transposition Cipher	48
2.5 Double Transposition	49
2.6 A 2-Step ADFGVX Cipher	52
2.7 An Approach to Decryption	53
2.8 Conclusions	56

3	Polyalphabetic Substitution Ciphers	59
3.1	Self-Reciprocal Ciphers	60
3.2	The Porta Polyalphabetic Cipher	60
3.3	The Beaufort Cipher	62
3.4	The Trithemius Cipher	63
3.5	The Vigenère Cipher	64
3.6	Breaking the Vigenère Cipher	66
3.7	Long Keys	72
3.8	A Variation on Vigenère	74
3.9	The Gronsfeld Cipher	75
3.10	Generating Permutations	76
3.11	The Eyraud Cipher	77
3.12	The Hill Cipher	80
3.13	The Jefferson Multiplex Cipher	82
3.14	Strip Ciphers	85
3.15	Polyphonic Ciphers and Ambiguity	85
3.16	Polybius's Polyalphabetic Cipher	87
3.17	The Index of Coincidence	88
4	Random Numbers	91
4.1	Manually Generated Random Numbers	92
4.2	True Random Numbers	93
4.3	Pseudo-Random Number Generators	97
4.4	Statistical Tests for Randomness	100
5	The Enigma	107
5.1	Rotor Machines	107
5.2	The Enigma: History	111
5.3	The Enigma: Operation	113
5.4	Breaking the Enigma Code	117
6	Stream Ciphers	131
6.1	Symmetric Key and Public Key	133
6.2	Stream Ciphers	134
6.3	Linear Shift Registers	136
6.4	Cellular Automata	139
6.5	Nonlinear Shift Registers	139
6.6	Other Stream Ciphers	145
6.7	Dynamic Substitution	145
6.8	The Latin Square Combiner	147
6.9	SEAL Stream Cipher	148
6.10	RC4 Stream Cipher	150

7	Block Ciphers	155
7.1	Block Ciphers	155
7.2	Lucifer	161
7.3	The Data Encryption Standard	162
7.4	Blowfish	175
7.5	IDEA	178
7.6	RC5	181
7.7	Rijndael	183
8	Public-Key Cryptography	195
8.1	Diffie–Hellman–Merkle Keys	195
8.2	Public-Key Cryptography	198
8.3	RSA Cryptography	199
8.4	Rabin Public-Key Method	203
8.5	El Gamal Public-Key Method	204
8.6	Pretty Good Privacy	205
8.7	Sharing Secrets: Threshold Schemes	206
8.8	The Four Components	212
8.9	Authentication	214
8.10	Elliptic Curve Cryptography	218
9	Quantum Cryptography	235
	Part II. Data Hiding	243
10	Data Hiding in Text	245
10.1	Basic Features	247
10.2	Applications of Data Hiding	250
10.3	Watermarking	251
10.4	Intuitive Methods	252
10.5	Simple Digital Methods	255
10.6	Data Hiding in Text	255
10.7	Innocuous Text	258
10.8	Mimic Functions	262
11	Data Hiding in Images	269
11.1	LSB Encoding	269
11.2	BPCS Steganography	280
11.3	Lossless Data Hiding	285
11.4	Spread Spectrum Steganography	294
11.5	Data Hiding by Quantization	297
11.6	Patchwork	298
11.7	Signature Casting in Images	299
11.8	Transform Domain Methods	301
11.9	Robust Data Hiding in JPEG Images	303
11.10	Robust Frequency Domain Watermarking	309
11.11	Detecting Malicious Tampering	312

xiv Contents

11.12	Wavelet Methods	314	
11.13	Kundur–Hatzinakos Watermarking: I	321	
11.14	Kundur–Hatzinakos Watermarking: II	323	
11.15	Data Hiding in Binary Images	325	
11.16	The Zhao–Koch Method	325	
11.17	The Wu–Lee Method	328	
11.18	The CPT Method	329	
11.19	The TP Method	332	
11.20	Data Hiding in Fax Images	336	
12	Data Hiding: Other Methods		339
12.1	Protecting Music Scores	339	
12.2	Data Hiding in MPEG-2 Video	341	
12.3	Digital Audio	344	
12.4	The Human Auditory System	347	
12.5	Audio Watermarking in the Time Domain	351	
12.6	Echo Hiding	353	
12.7	The Steganographic File System	356	
12.8	Ultimate Steganography?	361	
12.9	Public-Key Steganography	362	
12.10	Current Software	362	
Part III. Essential Resources			367
Appendixes			
A	Convolution		369
A.1	One-Dimensional Convolution	369	
A.2	Two-Dimensional Convolution	373	
B	Hashing		377
B.1	Hash Tables	377	
B.2	Hash Functions	378	
B.3	Collision Handling	379	
B.4	Secure Hash Functions	381	
C	Cyclic Redundancy Codes		383
D	Galois Fields		387
D.1	Field Definitions and Operations	387	
D.2	GF(256) and Rijndael	395	
D.3	Polynomial Arithmetic	399	
Answers to Exercises			401
Cryptography Timeline			419
Glossary			429
Bibliography			441
Index			453

Each memorable verse of a true poet has
two or three times the written content.

—Alfred de Musset



<http://www.springer.com/978-0-387-00311-5>

Data Privacy and Security

Salomon, D.

2003, XIV, 465 p. 45 illus., Hardcover

ISBN: 978-0-387-00311-5