

# Contents

<b>Preface</b>	<b>xi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Should You Read This Book?	2
1.2 Why Busy Ourselves With Cryptology?	3
1.2.1 'I've Nothing to Hide'	3
1.2.2 Cryptology: A Special Chain Link	7
1.3 What This Book Doesn't Cover—Another Story	11
<b>2 Cryptology from the Romans to World War II</b>	<b>17</b>
2.1 The Caesar Method and its Relatives	18
2.2 About Gold Bugs and Rhymes: Substitution and Transposition	20
2.2.1 Simple Substitution	20
2.2.2 First Improvement: Homophone Substitutions	25
2.2.3 What If I First Compressed the Text?	26
2.2.4 Transposition	28
2.2.5 Multiple Encryption	31
2.3 Combined Substitution: Digram Substitutions	32
2.4 Permanently Changing Tactics: Polyalphabetic Substitutions	35
2.4.1 The Vigenère Cipher	35
2.4.2 Bitwise Vigenère Method: Vernam Cipher	38

2.5	Domain of the Militaries: Ciphering Cylinders, Rotor Machines, and the Enigma	39
2.5.1	Structure and Significance of the Enigma	42
2.5.2	The Cryptanalysis of Enigma	45
2.5.3	The Enigma after 1945	53
2.6	The Only Safe Method: One-Time Pads	56
2.7	Bottom Line	59
<b>3</b>	<b>Cryptanalysis in Detail</b>	<b>61</b>
3.1	Aim and Methods. Some Basic Notions	62
3.2	Cryptanalytic Approaches	65
3.3	Example: <i>Crack</i> Finds UNIX Passwords	70
3.4	Back to Ciphering Cylinders	75
3.4.1	Negative Pattern Search	75
3.4.2	The Viaris Method	78
3.4.3	This is Still Interesting Today!	81
3.5	WordPerfect Encryption as a Modern Example	82
3.5.1	The Encryption Method: How to Find It, and How to Break It	82
3.5.2	The <i>newwpcrack</i> Program	85
3.6	The Vigenère Method Under the Magnifying Glass	91
3.6.1	The Index of Coincidence Supplies the Period Length. The Kasiski Method	91
3.6.2	Ciphertext Attack	94
3.6.3	The <i>vigcrack</i> Program	95
3.6.4	Compression = Compromise	102
3.7	<i>fcrypt</i> : How Differential Cryptanalysis Works	115
3.8	Bottom Line	121
<b>4</b>	<b>Development Milestones: DES, RSA</b>	<b>123</b>
4.1	Basic Terms	124
4.1.1	Bitwise Processing	124
4.1.2	Confusion and Diffusion	124
4.1.3	Stream Ciphers and Block Ciphers	126
4.1.4	Product Algorithms	127
4.1.5	The Image Is Gone, But We Still See It	129
4.2	Feistel Networks	132
4.3	The DES Method	133
4.3.1	A Difficult Labor	134

4.3.2	The Algorithm	135
4.4	How Secure is DES?	140
4.4.1	Brute-Force Attack and the ‘Deep Crack’ Computer	140
4.4.2	Differential Cryptanalysis—The Role of the S-Boxes	152
4.4.3	Attacking With Related Keys. Weak Keys	156
4.4.4	Linear Cryptanalysis and Other Methods	157
4.4.5	DFA and the Chip Crackers	162
4.4.6	Bottom Line	166
4.5	Asymmetric (Public-Key) Methods	167
4.5.1	Symmetric and Asymmetric Methods	167
4.5.2	Exchanging Keys With and Without a Public Key	169
4.5.3	The RSA Method and Eight Risks	176
4.5.4	The Knapsack Story	198
4.5.5	Bottom Line	202
<b>5</b>	<b>Life After DES: New Methods, New Attacks</b>	<b>205</b>
5.1	Implementation of Algorithms	205
5.1.1	Operating Modes: ECB, CBC, CFB, and OFB	206
5.1.2	Padding in Block Algorithms	216
5.1.3	Integrating Checksums	218
5.1.4	Generating Keys	219
5.1.5	Bottom Line	225
5.2	DES Modifications	225
5.2.1	Triple-DES	226
5.2.2	DES with Key-Dependent S-Boxes	229
5.2.3	DESX and Whitening	230
5.3	IDEA: A Special-Class Algorithm	232
5.3.1	This Time First: IDEA Patent Rights	232
5.3.2	The IDEA Method	233
5.3.3	Three Algebraic Operations Cleverly Linked	234
5.3.4	The IDEA Algorithm in Detail	236
5.3.5	Cryptanalyzing IDEA	239
5.3.6	Speed, Outlook	240
5.4	RC5: Yet Another Hope for DES Replacement	240
5.4.1	Description of the RC5 Algorithm	241
5.4.2	Cryptanalyzing RC5	244

5.4.3	The RC5a Modification	255
5.4.4	Patents and the RC6 Successor	258
5.5	Rijndael Becomes AES and Replaces DES	261
5.6	RC4: Stream Cipher for (Almost) Everyone	271
5.7	Other Interesting Methods	274
5.7.1	The <i>pkzip</i> Cipher and How to Break It	274
5.7.2	Classified Stuff in Air: The D-Networks and the A5 Algorithm	282
5.7.3	FEAL: The Cryptanalysts' Favorite	287
5.7.4	Other Algorithms: SEAL and Blowfish	288
5.7.5	NSA and Skipjack	291
5.8	Probabilistic and Quantum Cryptography	293
5.9	Quantum Computers. What's Still In There for Brute Force?	299
5.10	Surprise Attack From Behind: Timing and Power Analyses	306
5.11	What Is a Good Ciphering Method?	310
<b>6</b>	<b>Cryptographic Protocols</b>	<b>313</b>
6.1	Key Distribution	314
6.1.1	Diffie-Hellman, SKIP, KEA, and the Wide-Mouth Frog	314
6.1.2	Merkle's Riddle	322
6.1.3	Key Management and Authentication in GSM Networks	323
6.1.4	UMTS: People Learned Their Lessons	327
6.2	Sharing Secrets	330
6.2.1	Secret Splitting	330
6.2.2	Secret Sharing	331
6.2.3	Shared Secrets and Nuclear Fission	335
6.3	Digital Signatures	336
6.3.1	One-Way Hash Functions	336
6.3.2	Creating Digital Signatures	344
6.3.3	Security of Signatures	348
6.4	Key Escrow. Matt Blaze's Attack Against the EES Protocol	354
6.4.1	How Clipper and Capstone Work	354
6.4.2	How to Undermine the Protocol	356
6.5	One-Time Passwords	361

6.5.1	The Trick with One-Way Hash Functions	361
6.5.2	Attacks Against Your Bank Account	364
6.5.3	Password Tokens	368
6.6	Other Protocols	374
6.6.1	Timestamps	375
6.6.2	Bit Commitment	376
6.6.3	Blind Signatures	378
6.6.4	Zero-Knowledge Proofs	380
6.6.5	Fail-Stop Signatures	381
6.6.6	One-Way Accumulators	382
6.6.7	Electronic Money	383
6.6.8	The PIN on an ATM Card	389
6.6.9	Biometric Methods	394
6.7	Trojan Cryptography	400
<b>7</b>	<b>Practical Applications</b>	<b>409</b>
7.1	PGP—A King Among Cryptographic Programs	409
7.1.1	Phil Zimmermann, the NSA, and US Laws	410
7.1.2	What PGP Can Do	412
7.1.3	How PGP Works	416
7.1.4	PGP Versions—OpenPGP and GnuPG	421
7.1.5	A Tip for Working with Keyrings	427
7.2	PEM/RIPEM, the PGP Rival, and S/MIME	428
7.2.1	The PEM and S/MIME Standards Contra OpenPGP	428
7.2.2	RIPEM	432
7.2.3	Email Encryption in Practice: Disillusionment	433
7.3	Comfortable and Secure: SSH and OpenSSH	436
7.4	CFS-Encrypted Hard Disks	445
7.5	OPIE, S/Key, and Logdaemon: Secure Login	449
7.6	An RC5a Implementation	452
7.7	Bottom Line	457
<b>8</b>	<b>Cryptology, Politics, and Business</b>	<b>459</b>
8.1	The End of the Crypto-Monopoly	459
8.2	The Role of Politics Today	461
8.2.1	A Look Into the World of Intelligence Agencies	461
8.2.2	Privacy Shrinks	473
8.2.3	Key Escrow	477

8.2.4	Export Regulations and Patents	479
8.2.5	Digital Signatures	482
8.3	What Next?	483
<b>Glossary</b>		<b>487</b>
<b>Appendix A.1 Sources of Information</b>		<b>501</b>
<b>Appendix A.2 Bibliography</b>		<b>515</b>
<b>Index</b>		<b>527</b>