
Contents

Note to the Reader	xv
Introduction	xvii
Acknowledgments	xxv

Part I Classical Cryptology

1. Ancient Roots	3
1.1 Caveman Crypto	3
1.2 Greek Cryptography	4
1.2.1 Skytale Cipher	4
1.2.2 Polybius Cipher	5
1.3 Viking Cryptography	6
1.4 Early Steganography	7
References and Further Reading	8
2. Monalphabetic Substitution Ciphers, or MASCs:	
Disguises for Messages	11
2.1 Caesar Cipher	11
2.2 Other MASC Systems	12
2.3 Edgar Allan Poe	15
2.4 Arthur Conan Doyle	20
2.5 Frequency Analysis	22
2.6 Biblical Cryptology	25
2.7 More Frequencies and Pattern Words	26
2.8 Vowel Recognition Algorithms	30
2.8.1 Sukhotin's Method	30
2.9 More MASCs	33
2.10 Cryptanalysis of a MASC	36
2.11 Unsolved Ciphers by a Killer and a Composer	38
2.12 Affine Ciphers	41
2.13 Morse Code and Huffman Coding	46
2.14 MASC Miscellanea	51
2.15 Nomenclators	53
2.16 Cryptanalysis of Nomenclators	55
2.17 Book Codes	58
References and Further Reading	61

3. Simple Progression to an Unbreakable Cipher	69
3.1 Vigenère Cipher.....	69
3.2 History of the Vigenère Cipher	71
3.3 Cryptanalysis of the Vigenère Cipher.....	75
3.4 Kryptos.....	85
3.5 Autokeys.....	90
3.6 Running Key Cipher and Its Cryptanalysis.....	91
3.7 One-Time Pad or Vernam Cipher	103
3.8 Breaking the Unbreakable	106
3.9 Faking Randomness	110
3.10 Unsolved Cipher from 1915	113
3.11 OTPs and the SOE.....	113
3.12 History Rewritten!	114
References and Further Reading.....	115
4. Transposition Ciphers.....	119
4.1 Simple Rearrangements and Columnar Transposition.....	119
4.1.1 Rail-Fence Transposition	119
4.1.2 Rectangular Transposition	120
4.1.3 More Transposition Paths.....	122
4.2 Cryptanalysis of Columnar Transposition.....	124
4.3 Historic Uses.....	128
4.4 Anagrams.....	131
4.5 Double Transposition	134
4.6 Word Transposition	136
4.6.1 Civil War Reenactors.....	138
4.7 Transposition Devices	138
References and Further Reading.....	142
5. Shakespeare, Jefferson, and JFK	145
5.1 Shakespeare vs. Bacon.....	145
5.2 Thomas Jefferson: President, Cryptographer.....	150
5.3 Cipher Wheel Cryptanalysis	153
5.4 Playfair Cipher.....	166
5.5 Playfair Cryptanalysis.....	172
5.5.1 Computer Cryptanalysis	177
5.6 Kerckhoffs' Rules	178
References and Further Reading.....	180
6. World War I and Herbert O. Yardley	185
6.1 Zimmermann Telegram.....	185
6.2 ADFGX: A New Kind of Cipher.....	188
6.3 Cryptanalysis of ADFGX	190
6.4 Herbert O. Yardley	207
6.5 Peacetime Victory and a Tell-All Book.....	211
6.6 The Case of the Seized Manuscript.....	214

6.7	Cashing in, Again	214
6.8	Herbert O. Yardley: Traitor?	217
6.9	Censorship	219
	References and Further Reading.....	223
7.	Matrix Encryption.....	227
7.1	Levine and Hill.....	227
7.2	How Matrix Encryption Works	229
7.3	Levine's Attacks	231
7.4	Bauer and Millward's Attack.....	235
7.5	More Stories Left to Tell	240
	References and Further Reading.....	240
8.	World War II: The Enigma of Germany	245
8.1	Rise of the Machines.....	245
8.2	How Enigma Works.....	248
8.3	Calculating the Keyspace.....	254
8.4	Cryptanalysis Part 1. Recovering the Rotor Wirings.....	256
8.5	Cryptanalysis Part 2. Recovering the Daily Keys	274
8.6	After the Break	278
8.7	Alan Turing and Bletchley Park.....	278
8.8	Lorenz Cipher and Colossus	283
8.9	What if Enigma Had Never Been Broken?	285
8.10	Endings and New Beginnings	286
	References and Further Reading.....	289
9.	Cryptologic War against Japan.....	293
9.1	Forewarning of Pearl Harbor	293
9.2	Friedman's Team Assembles	294
9.3	Cryptanalysis of Red, a Japanese Diplomatic Cipher	296
9.3.1	Orange	301
9.4	Purple: How It Works	301
9.5	Purple Cryptanalysis.....	304
9.6	Practical Magic	307
9.7	Code Talkers	311
9.8	Code Talkers in Hollywood.....	319
9.9	Use of Languages as Oral Codes	321
	References and Further Reading.....	322

Part II Modern Cryptology

10.	Claude Shannon.....	329
10.1	About Claude Shannon.....	329
10.2	Entropy	330
10.3	One More Time.....	335
10.4	Unicity Points	337

10.5 Dazed and Confused.....	337
References and Further Reading.....	338
11. National Security Agency	341
11.1 Origins of NSA	342
11.2 TEMPEST.....	342
11.3 Size and Budget.....	345
11.4 The <i>Liberty</i> and the <i>Pueblo</i>	346
11.5 Church Committee Investigations	349
11.6 Post Cold War Downsizing	353
11.7 Some Speculation.....	354
11.8 2000 and Beyond	357
11.9 Interviewing with NSA.....	359
11.10 BRUSA, UKUSA, and Echelon.....	362
References and Further Reading.....	364
12. Data Encryption Standard	369
12.1 How DES Works.....	369
12.2 Reactions to and Cryptanalysis of DES	380
12.2.1 Objection 1: Key Size Matters.....	380
12.2.2 Objection 2: S-Box Secrecy.....	383
12.2.3 S-Boxes Revealed!	384
12.3 EFF vs. DES	385
12.4 Second Chance	388
12.5 Interesting Feature.....	390
12.5.1 Cryptologic Humor	393
12.6 Modes of Encryption.....	393
12.6.1 Levine's Methods.....	393
12.6.2 Modern Modes	395
References and Further Reading.....	399
13. Birth of Public Key Cryptography	403
13.1 Revolutionary Cryptologist.....	403
13.2 Diffie–Hellman Key Exchange.....	404
13.3 RSA: Solution from MIT.....	407
13.3.1 Fermat's Little Theorem (1640).....	409
13.3.2 Euclidean Algorithm	410
13.4 Government Control of Cryptologic Research	414
13.5 RSA Patented, Alice and Bob Born Free	422
References and Further Reading.....	424
14. Attacking RSA.....	427
14.1 Eleven Non-Factoring Attacks	427
14.1.1 Attack 1. Common Modulus Attack	427
14.1.2 Attack 2. Man-in-the-Middle	428
14.1.3 Attack 3. Low Decryption Exponent.....	429

14.1.4	Attack 4. Partial Knowledge of p or q	432
14.1.5	Attack 5. Partial Knowledge of d	432
14.1.6	Attack 6. Low Encryption Exponent Attack.....	432
14.1.7	Attack 7. Common Enciphering Exponent Attack.....	432
14.1.8	Attack 8. Searching the Message Space.....	435
14.1.9	Attack 9. Adaptive Chosen Ciphertext Attacks.....	435
14.1.10	Attack 10. Timing Attack.....	436
14.1.11	Attack 11. Ron Was Wrong, Whit Is Right Attack.....	437
14.2	Factoring Challenge.....	439
14.2.1	Old Problem.....	440
14.3	Trial Division and the Sieve of Eratosthenes (ca. 284–204 BCE)....	440
14.4	Fermat's Factorization Method.....	444
14.5	Euler's Factorization Method.....	445
14.6	Pollard's $p - 1$ Algorithm.....	447
14.7	Dixon's Algorithm.....	448
14.7.1	Quadratic Sieve.....	454
14.8	Pollard's Number Field Sieve.....	455
14.8.1	Other Methods.....	456
14.8.2	Cryptological Humor.....	456
	References and Further Reading.....	456
15.	Primality Testing and Complexity Theory.....	459
15.1	Some Facts about Primes.....	459
15.2	Fermat Test.....	462
15.3	Miller–Rabin Test.....	465
15.3.1	Generating Primes.....	467
15.4	Deterministic Tests for Primality.....	467
15.4.1	AKS Primality Test (2002).....	468
15.4.2	GIMPS.....	471
15.5	Complexity Classes, P vs. NP , Probabilistic vs. Deterministic.....	472
15.5.1	Cryptologic Humor.....	475
15.6	Ralph Merkle's Public Key Systems.....	475
15.7	Knapsack Encryption.....	479
15.8	Elgamal Encryption.....	482
	References and Further Reading.....	485
16.	Authenticity.....	489
16.1	Problem from World War II.....	489
16.2	Digital Signatures (and Some Attacks).....	490
16.2.1	Attack 12. Chosen Ciphertext Attack.....	492
16.2.2	Attack 13. Insider's Factoring Attack on the Common Modulus.....	492
16.2.3	Attack 14. Insider's Nonfactoring Attack.....	493
16.2.4	Elgamal Signatures.....	494
16.3	Hash Functions: Speeding Things Up.....	495

16.3.1	Rivest's MD5 and NIST's SHA-1	496
16.4	Digital Signature Algorithm	499
	References and Further Reading.....	501
17.	Pretty Good Privacy	503
17.1	Best of Both Worlds.....	503
17.2	Birth of PGP	504
17.3	In Zimmermann's Own Words.....	509
17.4	Impact of PGP.....	513
17.5	Implementation Issues	514
	References and Further Reading.....	516
18.	Stream Ciphers.....	519
18.1	Congruential Generators.....	519
18.2	Linear Feedback Shift Registers.....	521
18.3	LFSR Attack	523
18.4	Cellphone Stream Cipher A5/1	525
18.5	RC4	526
	References and Further Reading.....	529
19.	Suite B All-Stars.....	533
19.1	Elliptic Curve Cryptography.....	533
19.1.1	Elgamal, ECC Style	540
19.2	Personalities behind ECC	541
19.3	Advanced Encryption Standard (AES).....	543
19.3.1	SubBytes	546
19.3.2	ShiftRows	550
19.3.3	MixColumns.....	550
19.3.4	AddRoundKey	552
19.3.5	Putting It All Together: How AES-128 Works	553
19.4	AES Attacks	553
19.5	Security Guru Bruce Schneier.....	554
	References and Further Reading.....	555
20.	Possible Futures	559
20.1	Quantum Cryptography: How It Works	559
20.2	Quantum Cryptography: Historical Background.....	561
20.3	DNA Computing.....	566
	References and Further Reading.....	571
Index.....		575