

Contents

Part I: Cryptography	1
1 Introductory Synopsis	8
1.1 Cryptography and Steganography	8
1.2 Semagrams	9
1.3 Open Code: Masking	12
1.4 Cues	16
1.5 Open Code: Veiling by Nulls	18
1.6 Open Code: Veiling by Grilles	22
1.7 Classification of Cryptographic Methods	24
2 Aims and Methods of Cryptography	25
2.1 The Nature of Cryptography	25
2.2 Encryption	31
2.3 Cryptosystems	33
2.4 Polyphony	35
2.5 Character Sets	37
2.6 Keys	40
3 Encryption Steps: Simple Substitution	42
3.1 Case $V^{(1)} \dashrightarrow W$ (Unipartite Simple Substitutions)	42
3.2 Special Case $V \longleftrightarrow V$ (Permutations)	44
3.3 Case $V^{(1)} \dashrightarrow W^m$ (Multipartite Simple Substitutions)	51
3.4 The General Case $V^{(1)} \dashrightarrow W^{(m)}$, Straddling	53
4 Encryption Steps: Polygraphic Substitution and Coding .	56
4.1 Case $V^2 \dashrightarrow W^{(m)}$ (Digraphic Substitutions)	56
4.2 Special Cases of Playfair and Delastelle: Tomographic Methods....	62
4.3 Case $V^3 \dashrightarrow W^{(m)}$ (Trigraphic Substitutions)	66
4.4 The General Case $V^{(n)} \dashrightarrow W^{(m)}$: Codes	66
5 Encryption Steps: Linear Substitution	78
5.1 Self-reciprocal Linear Substitutions	80
5.2 Homogeneous Linear Substitutions	80
5.3 Binary Linear Substitutions	84
5.4 General Linear Substitutions	84

5.5	Decomposed Linear Substitutions	85
5.6	Decimated Alphabets	88
5.7	Linear Substitutions with Decimal and Binary Numbers	89
6	Encryption Steps: Transposition	91
6.1	Simplest Methods	91
6.2	Columnar Transpositions	95
6.3	Anagrams	98
7	Polyalphabetic Encryption: Families of Alphabets	101
7.1	Iterated Substitutions	101
7.2	Shifted and Rotated Alphabets	102
7.3	Rotor Crypto Machines	105
7.4	Shifted Standard Alphabets: Vigenère and Beaufort	114
7.5	Unrelated Alphabets	118
8	Polyalphabetic Encryption: Keys	126
8.1	Early Methods with Periodic Keys	126
8.2	‘Double Key’	128
8.3	Vernam Encryption	129
8.4	Quasi-nonperiodic Keys	131
8.5	Machines that Generate Their Own Key Sequences	132
8.6	Off-Line Forming of Key Sequences	143
8.7	Nonperiodic Keys	144
8.8	Individual, One-Time Keys	148
8.9	Key Negotiation and Key Management	151
9	Composition of Classes of Methods	155
9.1	Group Property	155
9.2	Superencryption	157
9.3	Similarity of Encryption Methods	159
9.4	Shannon’s ‘Pastry Dough Mixing’	160
9.5	Confusion and Diffusion by Arithmetical Operations	166
9.6	DES and IDEA	170
10	Open Encryption Key Systems	179
10.1	Symmetric and Asymmetric Encryption Methods	180
10.2	One-Way Functions	182
10.3	RSA Method	189
10.4	Cryptanalytic Attack upon RSA	191
10.5	Secrecy Versus Authentication	194
10.6	Security of Public Key Systems	196
11	Encryption Security	197
11.1	Cryptographic Faults	197
11.2	Maxims of Cryptology	205
11.3	Shannon’s Yardsticks	210
11.4	Cryptology and Human Rights	211

Part II: Cryptanalysis	217
12 Exhausting Combinatorial Complexity	220
12.1 Monoalphabetic Simple Encryptions	221
12.2 Monoalphabetic Polygraphic Encryptions	222
12.3 Polyalphabetic Encryptions	225
12.4 General Remarks on Combinatorial Complexity	227
12.5 Cryptanalysis by Exhaustion	227
12.6 Unicity Distance	229
12.7 Practical Execution of Exhaustion	231
12.8 Mechanizing the Exhaustion	234
13 Anatomy of Language: Patterns	235
13.1 Invariance of Repetition Patterns	235
13.2 Exclusion of Encryption Methods	237
13.3 Pattern Finding	238
13.4 Finding of Polygraphic Patterns	242
13.5 The Method of the Probable Word	242
13.6 Automatic Exhaustion of the Instantiations of a Pattern	247
13.7 Pangrams	249
14 Polyalphabetic Case: Probable Words	251
14.1 Non-Coincidence Exhaustion of Probable Word Position	251
14.2 Binary Non-Coincidence Exhaustion of Probable Word Position ..	254
14.3 The De Viaris Attack	255
14.4 Zig-Zag Exhaustion of Probable Word Position	263
14.5 The Method of Isomorphs	264
14.6 Covert Plaintext-Cryptotext Compromise	270
15 Anatomy of Language: Frequencies	271
15.1 Exclusion of Encryption Methods	271
15.2 Invariance of Partitions	272
15.3 Intuitive Method: Frequency Profile	274
15.4 Frequency Ordering	275
15.5 Cliques and Matching of Partitions	278
15.6 Optimal Matching	284
15.7 Frequency of Multigrams	286
15.8 The Combined Method of Frequency Matching	291
15.9 Frequency Matching for Polygraphic Substitutions	297
15.10 Free-Style Methods	298
15.11 Unicity Distance Revisited	299
16 Kappa and Chi	301
16.1 Definition and Invariance of Kappa	301
16.2 Definition and Invariance of Chi	304
16.3 The Kappa-Chi Theorem	306
16.4 The Kappa-Phi Theorem	307
16.5 Symmetric Functions of Character Frequencies	309

17	Periodicity Examination	311
17.1	The Kappa Test of Friedman	312
17.2	Kappa Test for Multigrams	313
17.3	Cryptanalysis by Machines	314
17.4	Kasiski Examination	320
17.5	Building a Depth and Phi Test of Kullback	326
17.6	Estimating the Period Length	329
18	Alignment of Accompanying Alphabets	331
18.1	Matching the Profile	331
18.2	Aligning Against Known Alphabet	335
18.3	Chi Test: Mutual Alignment of Accompanying Alphabets	339
18.4	Reconstruction of the Primary Alphabet	344
18.5	Kerckhoffs' Symmetry of Position	346
18.6	Stripping off Superencryption: Difference Method	351
18.7	Decryption of Code	354
18.8	Reconstruction of the Password	354
19	Compromises	356
19.1	Kerckhoffs' Superimposition	356
19.2	Superimposition for Encryptions with a Key Group	358
19.3	In-Phase Superimposition of Superencrypted Code	373
19.4	Cryptotext-Cryptotext Compromises	376
19.5	A Method of Sinkov	381
19.6	Cryptotext-Cryptotext Compromise: Doubling	388
19.7	Plaintext-Cryptotext Compromise: Feedback Cycle	402
20	Linear Basis Analysis	412
20.1	Reduction of Linear Polygraphic Substitutions	412
20.2	Reconstruction of the Key	413
20.3	Reconstruction of a Linear Shift Register	414
21	Anagramming	417
21.1	Transposition	417
21.2	Double Columnar Transposition	420
21.3	Multiple Anagramming	420
22	Concluding Remarks	423
22.1	Success in Breaking	424
22.2	Mode of Operation of the Unauthorized Decryptor	429
22.3	Illusory Security	434
22.4	Importance of Cryptology	435
	Appendix: Axiomatic Information Theory	438
	Bibliography	448
	Index	451
	Photo Credits	471