

Inhaltsverzeichnis

Teil I: Kryptographie	1
Die Leute	2
1 Einleitender Überblick	9
1.1 Kryptographie und Steganographie	9
1.2 Semagramme	10
1.3 Maskierung	14
1.4 Stichwörter	18
1.5 Verschleierung: Würfel	19
1.6 Verschleierung: Raster	24
1.7 Klassifizierung der kryptographischen Methoden	25
2 Aufgabe und Methode der Kryptographie	27
2.1 Charakter der Kryptographie	27
2.2 Chiffrierung	34
2.3 Chiffrierschritt-System	35
2.4 Polyphonie	38
2.5 Zeichenvorräte	40
2.6 Schlüssel	42
3 Chiffrierschritte: Einfache Substitution	46
3.1 Fall $V^{(1)} \dashrightarrow W$ (unipartite einfache Substitutionen)	46
3.2 Spezialfall $V \longleftrightarrow V$ (Permutationen)	48
3.3 Fall $V^{(1)} \dashrightarrow W^m$ (multipartite einfache Substitutionen)	55
3.4 Der allgemeine Fall $V^{(1)} \dashrightarrow W^{(m)}$, Spreizen	57
4 Chiffrierschritte: Polygraphische Substitution und Codierung	60
4.1 Der Fall $V^2 \dashrightarrow W^{(m)}$ von Bigramm-Substitutionen	60
4.2 Spezialfälle von Playfair und Delastelle: Tomographische Verfahren	66
4.3 Der Fall $V^3 \dashrightarrow W^{(m)}$ von Trigramm-Substitutionen	69
4.4 Der allgemeine Fall $V^{(n)} \dashrightarrow W^{(m)}$: Codes	70
5 Chiffrierschritte: Lineare Substitution	82
5.1 Involutorische lineare Substitutionen	84
5.2 Homogene und inhomogene lineare Substitutionen	84
5.3 Binäre lineare Substitutionen	88
5.4 Allgemeine lineare Substitutionen	88
5.5 Zerfallende lineare Substitutionen	89

5.6	Dezimierte Alphabete	92
5.7	Lineare Substitutionen mit Dezimalzahlen und Dualzahlen	93
6	Chiffrierschritte: Transposition	95
6.1	Einfachste Verfahren	95
6.2	Spalten-Transpositionen	99
6.3	Anagramme	104
7	Polyalphabetische Chiffrierung: Begleitende und unabhängige Alphabete	107
7.1	Potenzierung	107
7.2	Verschobene und rotierte Alphabete	108
7.3	Rotor-Maschinen	112
7.4	Verschobene Standardalphabete: Vigenère und Beaufort	121
7.5	Unabhängige Alphabete	125
8	Polyalphabetische Chiffrierung: Schlüssel	133
8.1	Frühe Verfahren mit periodischen Schlüsseln	133
8.2	„Doppelter Schlüssel“	135
8.3	Vernam-Chiffrierung	136
8.4	Quasi-nichtperiodische Schlüssel	138
8.5	Maschinen mit eingebauten Schlüsselerzeugern	139
8.6	Bildung von Schlüsselfolgen durch Iteration	151
8.7	Nichtperiodische Schlüssel	152
8.8	Individuelle Einmal-Schlüssel	156
8.9	Schlüsselverwaltung	160
9	Komposition von Chiffrierverfahren	164
9.1	Gruppeneigenschaft	164
9.2	Überchiffrierung	167
9.3	Ähnlichkeit von Chiffrierverfahren	169
9.4	Durchmischung nach Shannon	169
9.5	Durchmischung durch arithmetische Operationen	176
9.6	DES und IDEA®	180
10	Öffentliche Chiffrierschlüssel	190
10.1	Symmetrische und asymmetrische Chiffrierverfahren	191
10.2	Einweg-Funktionen	194
10.3	RSA-Verfahren	201
10.4	Anmerkungen zur Sicherheit von RSA	203
10.5	Geheimhaltung versus Authentisierung	208
10.6	Sicherheit der öffentlichen Chiffrierverfahren	209
11	Chiffriersicherheit	211
11.1	Chiffrierfehler	211
11.2	Maximen der Kryptologie	220
11.3	Shannons Maßstäbe	227
11.4	Kryptologie und Grundrechte	228

Teil II: Kryptanalyse	235
Die Maschinerie	236
12 Ausschöpfung der kombinatorischen Komplexität	238
12.1 Monoalphabetische einfache Chiffrierungen	239
12.2 Monoalphabetische polygraphische Chiffrierungen	240
12.3 Polyalphabetische Chiffrierungen	242
12.4 Allgemeine Bemerkungen	244
12.5 Die Exhaustionsmethode	245
12.6 Unizitätslänge	247
12.7 Praktische Durchführung der Exhaustion	249
12.8 Mechanisierung der Exhaustion	252
13 Anatomie der Sprache: Muster	253
13.1 Invarianz der Wiederholungsmuster	253
13.2 Ausschließung von Chiffrierverfahren	256
13.3 Mustersuche	256
13.4 Mustersuche bei polygraphischer Chiffrierung	260
13.5 Die Methode des wahrscheinlichen Wortes	261
13.6 Maschinelle Exhaustion der Belegungen eines Musters	266
13.7 Pangramme	268
14 Polyalphabetischer Fall: Wahrscheinliche Wörter	270
14.1 Negative Mustersuche	270
14.2 Binäre negative Mustersuche bei Porta-Alphabeten	273
14.3 Mustersuche bei bekannten Alphabeten — De Viaris	274
14.4 Zick-Zack-Exhaustion möglicher Wortlagen	282
14.5 Isomorphie-Methode	284
14.6 Verdeckte Klartext-Geheimtext-Kompromittierung	291
15 Anatomie der Sprache: Häufigkeit	292
15.1 Ausschließung von Chiffrierverfahren	292
15.2 Invarianz der Partitionen	293
15.3 Intuitive Häufigkeitserkennung: Häufigkeitsgebirge	294
15.4 Häufigkeitsreihenfolge	296
15.5 Cliques und Partitionsanpassung	299
15.6 Abstandsminimierung	305
15.7 Häufigkeit von Multigrammen	307
15.8 Die kombinierte Methode der Häufigkeitserkennung	312
15.9 Häufigkeitserkennung für polygraphische Substitutionen	318
15.10 Freistil-Methoden	319
15.11 Nochmals: Unizitätslänge	321
16 Kappa und Chi	323
16.1 Definition und Invarianz von Kappa	323
16.2 Definition und Invarianz von Chi und Psi	326
16.3 Das Kappa-Chi-Theorem	329

16.4	Das Kappa-Phi-Theorem	330
16.5	Symmetrische Funktionen der Zeichenhäufigkeiten	331
17	Periodenanalyse	333
17.1	Friedmans Periodenbestimmung durch Kappa-Test	334
17.2	Kappa-Test für Multigramme	336
17.3	Maschinelle Kryptanalyse	338
17.4	Parallelstellensuche nach Kasiski	343
17.5	Kolonnenbildung und Phi-Test nach Kullback	348
17.6	Eine Abschätzung für die Periodenlänge	351
18	Zurechtrücken begleitender Alphabete	353
18.1	Durchdecken der Häufigkeitsgebirge	353
18.2	Chi-Test: Zurechtrücken gegen bekanntes Alphabet	357
18.3	Chi-Test: Gegenseitiges Zurechtrücken begleitender Alphabete ...	361
18.4	Wiedergewinnung des Referenzalphabets	366
18.5	Kerckhoffs' symétrie de position	368
18.6	Abstreifen einer Überchiffrierung: Differenzenmethode	374
18.7	Entziffern des Codes	376
18.8	Rekonstruktion des Kennwortes	376
19	Kompromittierung	378
19.1	Kerckhoffs' Superimposition	378
19.2	Superimposition für Chiffrierungen mit einer Schlüsselgruppe ...	380
19.3	Phasenrichtige Superimposition von überchiffriertem Code	396
19.4	Geheimtext-Geheimtext-Kompromittierung	399
19.5	Eine Methode von Sinkov	403
19.6	Geheimtext-Geheimtext-Kompromittierung: Indikatorverdopplung	411
19.7	Klartext-Geheimtext-Kompromittierung: Rückkoppelpläne	426
20	Lineare Basisanalyse	436
20.1	Reduktion linearer polygraphischer Substitutionen	436
20.2	Rekonstruktion eines durch lineare Iteration erzeugten Schlüssels	437
20.3	Rekonstruktion eines linearen Schieberegisters	438
21	Anagrammieren	441
21.1	Einfache Transposition	441
21.2	Doppelte Spaltentransposition	444
21.3	Multiples Anagrammieren	444
22	Abschließende Bemerkungen	447
22.1	Geglückte Entzifferungen	448
22.2	Arbeitsweise des unbefugten Entzifferers	454
22.3	Illusion der Sicherheit	459
22.4	Kommunikationstheoretische Bedeutung der Kryptologie	461

A	Anhang: Perfekte Sicherheit und praktische Sicherheit ..	464
A.1	Axiome einer axiomatischen Informationstheorie	464
A.2	Informationstheorie von Chiffrierungen	466
A.3	Perfekte und individuelle Chiffrierungen	468
A.4	Shannonscher Hauptsatz	470
A.5	Unizitätslänge und Codekomprimierung	471
A.6	Unmöglichkeit einer konstruktiven vollständigen Unordnung	473
B	Anhang: Kryptologische Geräte und Maschinen	
	im Deutschen Museum München	475
	Literatur	478
	Namen- und Sachverzeichnis	481
	Bildquellenverzeichnis	503

<http://www.springer.com/978-3-540-67931-8>

Entzifferte Geheimnisse

Methoden und Maximen der Kryptologie

Bauer, F.L.

2000, XIV, 503 S. 193 Abb., 17 Abb. in Farbe.,

Hardcover

ISBN: 978-3-540-67931-8