

Inhaltsverzeichnis

Teil I: Kryptographie	1
1 Einleitender Überblick	5
1.1 Kryptographie und Steganographie	5
1.2 Maskierung	8
1.3 Stichworte	13
1.4 Unsichtbare Tarnung	14
1.5 Raster	18
2 Aufgabe und Methode der Kryptographie	21
2.1 Charakter der Kryptographie	21
2.2 Chiffrierung	26
2.3 Chiffriersystem	27
2.4 Polyphonie	29
2.5 Zeichenvorräte	31
2.6 Schlüssel	33
3 Chiffrierschritte: Einfache Substitution	35
3.1 Spezialfall $V^{(1)} \dashrightarrow W^{(1)}$	36
3.2 Spezialfall $V \longleftrightarrow V$	37
3.3 Fall $V^{(1)} \dashrightarrow W^m, m > 1$	43
3.4 Der allgemeine Fall $V^{(1)} \dashrightarrow W^{(m)}$, Spreizen	45
4 Chiffrierschritte: Polygraphische Substitution und Codierung	48
4.1 Der Fall $V^2 \dashrightarrow W^{(m)}$ von Bigramm-Substitutionen	48
4.2 Spezialfälle von Playfair und Delastelle: tomographische Verfahren	51
4.3 Der Fall $V^3 \dashrightarrow W^{(m)}$ von Trigramm-Substitutionen	54
4.4 Der allgemeine Fall $V^{(n)} \dashrightarrow W^{(m)}$; Codes	54
5 Chiffrierschritte: Lineare Substitution	62
5.1 Involutorische lineare Substitutionen	63
5.2 Homogene und inhomogene lineare Substitutionen	64
5.3 Binäre lineare Substitutionen	67

5.4	Allgemeine lineare Substitutionen	67
5.5	Zerfallende lineare Substitutionen	68
5.6	Übergreifende Alphabete	69
5.7	<i>n</i> -ziffrige Dezimalzahlen	70
6	Chiffrierschritte: Transposition	73
6.1	Einfachste Verfahren	73
6.2	Spalten-Transpositionen	76
6.3	Anagramme	78
7	Polyalphabetische Chiffrierung: Begleitende Alphabete ...	82
7.1	Potenzierung	82
7.2	Verschobene und rotierte Alphabete	83
7.3	Verschobene Standardalphabete: Vigenère und Beaufort	88
7.4	Unabhängige Alphabete	91
8	Polyalphabetische Chiffrierung: Schlüssel	98
8.1	Frühe Verfahren mit periodischen Schlüsseln	98
8.2	„Doppelter Schlüssel“	100
8.3	Vernam-Chiffrierung	101
8.4	Quasi-nichtperiodische Schlüssel	102
8.5	Fortlaufende Schlüssel	106
8.6	Fortlaufende individuelle Schlüssel	109
9	Komposition von Verfahrensklassen	112
9.1	Gruppeneigenschaft	112
9.2	Überchiffrierung	114
9.3	Ähnlichkeit von Chiffriersystemen	114
9.4	Durchmischung nach <i>Shannon</i>	114
9.5	Tomographische Verfahren	120
9.6	DES	121
9.7	Durchmischung durch arithmetische Operationen	127
10	Chiffriersicherheit	130
10.1	Chiffrierfehler	130
10.2	Maximen der Kryptologie	136
10.3	Shannons Maßstäbe	140
11	Öffentliche Schlüssel	141
11.1	Symmetrische und asymmetrische Chiffrierverfahren	142
11.2	Einweg-Funktionen	144
11.3	RSA-Verfahren	148
11.4	Anmerkungen zur Sicherheit von RSA	150
11.5	Das Verfahren von ElGamal	154
11.6	Authentisierung	154
11.7	Diskussion	155

Teil II: Kryptanalyse	157
12 Ausschöpfung der kombinatorischen Komplexität	159
12.1 Einfache monoalphabetische Substitutionen	160
12.2 Polygraphische monoalphabetische Substitutionen	161
12.3 Polyalphabetische monographische Substitutionen	163
12.4 Allgemeine Bemerkungen	166
12.5 Die Exhaustionsmethode	166
12.6 Unizitätslänge	168
12.7 Praktische Durchführung der Exhaustion	170
12.8 Mechanisierung der Exhaustion	173
12.9 Exhaustion bei polyphoner Chiffrierung	173
13 Anatomie der Sprache: Muster	174
13.1 Invarianz der Wiederholungsmuster	174
13.2 Ausschließung von Chiffrierverfahren	175
13.3 Intuitive Mustererkennung	175
13.4 Mustererkennung bei polygraphischer Chiffrierung	180
13.5 Die Methode des wahrscheinlichen Wortes	181
13.6 Maschinelle Exhaustion der Belegungen eines Musters	184
13.7 Pangramme	187
14 Muster im polyalphabetischen Fall	189
14.1 Negative Mustersuche	189
14.2 Binäre Mustersuche bei Porta-Alphabeten	192
14.3 Mustersuche bei bekannten Alphabeten — De Viaris	192
14.4 Geheimtext-Klartext-Kompromittierung	199
15 Anatomie der Sprache: Häufigkeit	201
15.1 Ausschließung von Chiffrierverfahren	201
15.2 Invarianz der Partitionen	202
15.3 Intuitive Häufigkeitserkennung: Häufigkeitsgebirge	203
15.4 Häufigkeitsreihenfolge	205
15.5 Cliques und Partitionsanpassung	208
15.6 Abstandsminimierung	217
15.7 Häufigkeit von n -grammen	218
15.8 Die kombinierte Methode der Häufigkeitserkennung	224
15.9 Häufigkeitserkennung für polygraphische Substitutionen	229
15.10 Freistil-Methoden	232
15.11 Nochmals: Unizitätslänge	233
16 Kappa und Chi	235
16.1 Definition und Invarianz von Kappa	235
16.2 Definition und Invarianz von Chi	238
16.3 Das Kappa-Chi-Theorem	241
16.4 Das Kappa-Phi-Theorem	242
16.5 Symmetrische Funktionen der Zeichenhäufigkeiten	243

17	Periodenanalyse	245
17.1	Friedmans Periodenbestimmung durch Kappa-Verlauf	246
17.2	Kappa-Verlauf für Multigramme	247
17.3	Parallelstellensuche nach Kasiski	251
17.4	Kolonnenbildung und Phi-Test nach Kullback	256
17.5	Eine Abschätzung für die Periodenlänge	260
18	Zurechtrücken begleitender Alphabete	261
18.1	Durchdecken der Häufigkeitsgebirge	261
18.2	Zurechtrücken gegen bekanntes Alphabet	265
18.3	Gegenseitiges Zurechtrücken begleitender Alphabete	269
18.4	Wiedergewinnung des Referenzalphabets	272
18.5	Kerckhoffs' <i>symétrie de position</i>	276
18.6	Abstreifen einer Überchiffrierung: Differenzenmethode	281
18.7	Entziffern des Codes	284
18.8	Rekonstruktion des Kennwortes	284
19	Superimposition	286
19.1	Kerckhoffs' <i>superimposition</i>	286
19.2	Phasenrichtige Superimposition von überchiffriertem Code	288
19.3	Geheimtext-Geheimtext-Kompromittierung	290
19.4	Geheimtext-Geheimtext-Kompromittierung bei der Rotor-Chiffrierung	300
19.5	Geheimtext-Klartext-Kompromittierung bei der Rotor-Chiffrierung	311
20	Lineare Basisanalyse	316
20.1	Reduktion linearer polygraphischer Substitutionen	316
20.2	Rekonstruktion eines durch lineare Iteration erzeugten Schlüssels	317
20.3	Rekonstruktion eines linearen Schieberegisters	318
21	Anagrammieren	321
21.1	Einfache Transposition	321
21.2	Doppelte Spaltentransposition	324
21.3	Multiples Anagrammieren	324
22	Abschließende Bemerkungen	327
22.1	Arbeitsweise des unberufenen Entzifferers	328
22.2	Perfekte Sicherheit und praktische Sicherheit	331
22.3	Unmöglichkeit einer vollständigen Unordnung	337
22.4	Bedeutung der Kryptologie	338
	Anhang: Kryptologische Geräte und Maschinen im Deutschen Museum München	339
	Literatur	342
	Namen- und Sachverzeichnis	345