

Friedrich L. Bauer

# Entzifferte Geheimnisse

Methoden und Maximen  
der Kryptologie

Mit 159 Abbildungen und 10 Farbtafeln



Springer

# Inhaltsverzeichnis

<b>Teil I: Kryptographie</b> .....	1
<b>1 Einleitender Überblick</b> .....	5
1.1 Kryptographie und Steganographie .....	5
1.2 Maskierung .....	8
1.3 Stichworte .....	13
1.4 Unsichtbare Tarnung .....	14
1.5 Raster .....	18
<b>2 Aufgabe und Methode der Kryptographie</b> .....	21
2.1 Charakter der Kryptographie .....	21
2.2 Chiffrierung .....	26
2.3 Chiffriersystem .....	27
2.4 Polyphonie .....	30
2.5 Zeichenvorräte .....	32
2.6 Schlüssel .....	34
<b>3 Chiffrierschritte: Einfache Substitution</b> .....	36
3.1 Fall $V^{(1)} \dashrightarrow W$ (monopartite einfache Substitution) .....	37
3.2 Spezialfall $V \longleftrightarrow V$ .....	38
3.3 Fall $V^{(1)} \dashrightarrow W^m$ , $m > 1$ .....	44
3.4 Der allgemeine Fall $V^{(1)} \dashrightarrow W^{(m)}$ , Spreizen .....	47
<b>4 Chiffrierschritte: Polygraphische Substitution und Codierung</b> .....	50
4.1 Der Fall $V^2 \dashrightarrow W^{(m)}$ von Bigramm-Substitutionen .....	50
4.2 Spezialfälle von Playfair und Delastelle: tomographische Verfahren .....	54
4.3 Der Fall $V^3 \dashrightarrow W^{(m)}$ von Trigramm-Substitutionen .....	57
4.4 Der allgemeine Fall $V^{(n)} \dashrightarrow W^{(m)}$ : Codes .....	58
<b>5 Chiffrierschritte: Lineare Substitution</b> .....	66
5.1 Involutorische lineare Substitutionen .....	68
5.2 Homogene und inhomogene lineare Substitutionen .....	68
5.3 Binäre lineare Substitutionen .....	72

5.4	Allgemeine lineare Substitutionen .....	72
5.5	Zerfallende lineare Substitutionen .....	73
5.6	Übergreifende Alphabete .....	74
5.7	$n$ -ziffrige Dezimalzahlen und Dualzahlen .....	74
6	<b>Chiffrierschritte: Transposition</b> .....	78
6.1	Einfachste Verfahren .....	78
6.2	Spalten-Transpositionen .....	81
6.3	Anagramme .....	84
7	<b>Polyalphabetische Chiffrierung: Begleitende Alphabete</b> ...	87
7.1	Potenzierung .....	87
7.2	Verschobene und rotierte Alphabete .....	88
7.3	Verschobene Standardalphabete: Vigenère und Beaufort .....	94
7.4	Unabhängige Alphabete .....	97
8	<b>Polyalphabetische Chiffrierung: Schlüssel</b> .....	105
8.1	Frühe Verfahren mit periodischen Schlüsseln .....	105
8.2	„Doppelter Schlüssel“ .....	107
8.3	Vernam-Chiffrierung .....	108
8.4	Quasi-nichtperiodische Schlüssel .....	109
8.5	Fortlaufende Schlüssel .....	114
8.6	Fortlaufende individuelle Schlüssel .....	117
9	<b>Komposition von Verfahrensklassen</b> .....	120
9.1	Gruppeneigenschaft .....	120
9.2	Überchiffrierung .....	122
9.3	Ähnlichkeit von Chiffriersystemen .....	123
9.4	Durchmischung nach <i>Shannon</i> .....	123
9.5	Tomographische Verfahren .....	129
9.6	DES .....	130
9.7	Durchmischung durch arithmetische Operationen .....	136
10	<b>Chiffriersicherheit</b> .....	139
10.1	Chiffrierfehler .....	139
10.2	Maximen der Kryptologie .....	147
10.3	Shannons Maßstäbe .....	152
11	<b>Öffentliche Schlüssel</b> .....	153
11.1	Symmetrische und asymmetrische Chiffrierverfahren .....	154
11.2	Einweg-Funktionen .....	156
11.3	RSA-Verfahren .....	160
11.4	Anmerkungen zur Sicherheit von RSA .....	162
11.5	Das Verfahren von ElGamal .....	166
11.6	Authentisierung .....	166
11.7	Diskussion .....	167

<b>Teil II: Kryptanalyse</b> .....	169
<b>12 Ausschöpfung der kombinatorischen Komplexität</b> .....	171
12.1 Monoalphabetische einfache Chiffrierungen .....	172
12.2 Monoalphabetische polygraphische Chiffrierungen .....	173
12.3 Polyalphabetische Chiffrierungen .....	176
12.4 Allgemeine Bemerkungen .....	178
12.5 Die Exhaustionsmethode .....	178
12.6 Unizitätslänge .....	180
12.7 Praktische Durchführung der Exhaustion .....	182
12.8 Mechanisierung der Exhaustion .....	185
12.9 Exhaustion möglicher Lagen eines Wortes .....	185
<b>13 Anatomie der Sprache: Muster</b> .....	186
13.1 Invarianz der Wiederholungsmuster .....	186
13.2 Ausschließung von Chiffrierverfahren .....	187
13.3 Intuitive Mustererkennung .....	187
13.4 Mustererkennung bei polygraphischer Chiffrierung .....	192
13.5 Die Methode des wahrscheinlichen Wortes .....	193
13.6 Maschinelle Exhaustion der Belegungen eines Musters .....	197
13.7 Pangramme .....	200
<b>14 Muster im polyalphabetischen Fall</b> .....	201
14.1 Negative Mustersuche .....	201
14.2 Binäre Mustersuche bei Porta-Alphabeten .....	204
14.3 Mustersuche bei bekannten Alphabeten — De Viaris .....	204
14.4 Klartext-Geheimtext-Kompromittierung .....	211
<b>15 Anatomie der Sprache: Häufigkeit</b> .....	213
15.1 Ausschließung von Chiffrierverfahren .....	213
15.2 Invarianz der Partitionen .....	214
15.3 Intuitive Häufigkeitserkennung: Häufigkeitsgebirge .....	215
15.4 Häufigkeitsreihenfolge .....	217
15.5 Cliques und Partitionsanpassung .....	220
15.6 Abstandsminimierung .....	229
15.7 Häufigkeit von $n$ -grammen .....	230
15.8 Die kombinierte Methode der Häufigkeitserkennung .....	236
15.9 Häufigkeitserkennung für polygraphische Substitutionen .....	241
15.10 Freistil-Methoden .....	244
15.11 Nochmals: Unizitätslänge .....	245
<b>16 Kappa und Chi</b> .....	247
16.1 Definition und Invarianz von Kappa .....	247
16.2 Definition und Invarianz von Chi .....	250
16.3 Das Kappa-Chi-Theorem .....	253
16.4 Das Kappa-Phi-Theorem .....	254
16.5 Symmetrische Funktionen der Zeichenhäufigkeiten .....	255

17	<b>Periodenanalyse</b> .....	257
17.1	Friedmans Periodenbestimmung durch Kappa-Verlauf .....	258
17.2	Kappa-Verlauf für Multigramme .....	259
17.3	Parallelstellensuche nach Kasiski .....	263
17.4	Kolonnenbildung und Phi-Test nach Kullback .....	268
17.5	Eine Abschätzung für die Periodenlänge .....	272
18	<b>Zurechtrücken begleitender Alphabete</b> .....	273
18.1	Durchdecken der Häufigkeitsgebirge .....	273
18.2	Zurechtrücken gegen bekanntes Alphabet .....	277
18.3	Gegenseitiges Zurechtrücken begleitender Alphabete .....	281
18.4	Wiedergewinnung des Referenzalphabets .....	286
18.5	Kerckhoffs' <i>symétrie de position</i> .....	288
18.6	Abstreifen einer Überchiffrierung: Differenzenmethode .....	293
18.7	Entziffern des Codes .....	296
18.8	Rekonstruktion des Kennwortes .....	297
19	<b>Kompromittierung</b> .....	299
19.1	Kerckhoffs' <i>superimposition</i> .....	299
19.2	Superimposition für Chiffrierungen mit einer Schlüsselgruppe ...	301
19.3	Phasenrichtige Superimposition von überchiffriertem Code ....	312
19.4	Geheimtext-Geheimtext-Kompromittierung .....	315
19.5	Eine Methode von Sinkov .....	318
19.6	Geheimtext-Geheimtext-Kompromittierung: Textverdopplung ..	325
19.7	Klartext-Geheimtext-Kompromittierung: Koppelpläne .....	339
19.8	Verschaltung der ENIGMA-Rotoren .....	345
20	<b>Lineare Basisanalyse</b> .....	346
20.1	Reduktion linearer polygraphischer Substitutionen .....	346
20.2	Rekonstruktion eines durch lineare Iteration erzeugten Schlüssels .....	347
20.3	Rekonstruktion eines linearen Schieberegisters .....	348
21	<b>Anagrammieren</b> .....	351
21.1	Einfache Transposition .....	351
21.2	Doppelte Spaltransposition .....	354
21.3	Multiples Anagrammieren .....	354
22	<b>Abschließende Bemerkungen</b> .....	357
22.1	Arbeitsweise des unberufenen Entzifferers .....	358
22.2	Bedeutung der Kryptologie .....	362
	<b>Anhang: Perfekte Sicherheit und praktische Sicherheit</b> .....	364
	<b>Anhang: Kryptologische Geräte und Maschinen im Deutschen Museum München</b> .....	372
	<b>Literatur</b> .....	375
	<b>Namen- und Sachverzeichnis</b> .....	378