

Michael Miller

Symmetrische Verschlüsselungs- verfahren

**Design, Entwicklung und
Kryptoanalyse klassischer
und moderner Chiffren**



Teubner

B.G.Teubner Stuttgart • Leipzig • Wiesbaden

Inhaltsverzeichnis

Kryptoanalyse klassischer Chiffrierverfahren	1
1.1 Einleitung	2
1.2 Elemente der Verschlüsselung	4
1.3 Monoalphabetische Substitutionschiffren.	7
1.4 Analyse monoalphabetischer Chiffren.	10
1.5 Beispiel: Analyse einer monoalphabetischen Chiffre.	13
1.6 Polyalphabetische Chiffrierverfahren.	20
1.7 Kasiski-Test	25
1.8 Koinzidenzindex von Friedman.	27
1.9 Beispiel: Analyse einer polyalphabetischen Chiffre.	34
1.10 Permutationschiffren.	38
Die Kryptoanalyse der „Enigma“-Chiffre	43
2.1 Entwicklung kryptographischer Geräte zu Beginn des 20. Jahr- hunderts	44
2.2 Prinzip der Rotorchiffrierung	49
2.3 Arbeitsweise der Wehrmachtsenigma	51
2.4 Enigma-Schlüsselverfahren im zweiten Weltkrieg	55
2.5 Polnische Analysen — 1926 bis 1939.	57
2.6 Britische Analysen — 1939 bis 1945.	64
Shannons Theorie der Kryptosysteme	73
3.1 Hintergrund und Notation.	74
3.2 Stochastische Modellierung	78
3.3 Perfekte Chiffren — absolute Sicherheit	81
3.4 Das One-Time-Pad	84
3.5 Entropie	88
3.6 Theorie der Kryptosysteme.	105
3.7 Konfusion und Diffusion.	111
Lucifer-Chiffre und der Data Encryption Standard	115
4.1 Grundlagen	116
4.2 Die Lucifer-Algorithmen	120
4.3 Struktur einer Feistel-Chiffre.	127

4.4	Geschichte des DES	130
4.5	Beschreibung des DES-Algorithmus	133
4.6	Beispiel einer DES-Verschlüsselung	144
4.7	Betriebsarten einer Blockchiffre	147
Differentielle Kryptoanalyse		149
5.1	Einleitung — Motivation	150
5.2	Übersicht zur Vorgehensweise der differentiellen Kryptoanalyse	151
5.3	Grundlagen	154
5.4	Analyse einer DES-Rundenfunktion	158
5.5	Analyse des DES mit drei Runden	163
5.6	Analyse des DES mit mehreren Runden	164
5.7	Schlüsselbestimmung mit Hilfe der Charakteristik	172
5.8	Differentielle Kryptoanalyse des DES mit sechs Runden	174
5.9	Aufwandsanalyse und Aufwandsreduzierung	176
5.10	Resultate der differentiellen Kryptoanalyse	182
Lineare Kryptoanalyse		187
6.1	Einleitung — Motivation	188
6.2	Grundlagen	188
6.3	Übersicht zur Vorgehensweise der linearen Approximation	194
6.4	Analyse des DES mit drei Runden	202
6.5	Analyse des DES mit fünf Runden	204
6.6	Analyse des DES mit acht Runden	207
6.7	Analyse des DES mit mehr als acht Runden	216
6.8	Aufwand und Erfolgswahrscheinlichkeit der linearen Analyse	218
Advanced Encryption Standard		223
7.1	Geschichte des AES	224
7.2	Grobstruktur des Verschlüsselungsalgorithmus	227
7.3	Notation	230
7.4	Mathematische Grundlagen	232
7.5	Beschreibung der einzelnen Verschlüsselungsschritte	236
7.6	Struktur des Entschlüsselungsalgorithmus	242
7.7	Auswahl der Rundenschlüssel	249
7.8	Beispiel einer AES-Verschlüsselung	253
Mathematische Grundlagen		255
8.1	Zahlentheorie	255
8.1.1	Natürliche Zahlen und ganze Zahlen	256
8.1.2	Modulare Arithmetik	256
8.2	Algebra	257
8.2.1	Gruppen	257
8.2.2	Ringe	259
8.2.3	Körper	260
8.2.4	Polynomringe	262