

Klaus Schmeh

Codeknacker gegen Codemacher

Die faszinierende Geschichte der
Verschlüsselung

Mit einem Geleitwort von
Prof. Dr. C. Paar

Inhalt

1	Das Zeitalter der Verschlüsselung von Hand	1
1.1	Als die Schrift zum Rätsel wurde.....	1
1.2	Der Telegrafie-Schub.....	10
1.3	Ein Weltkrieg der geheimen Zeichen.....	17
1.4	Room 40	23
1.5	Auf dem Weg zur kryptologischen Weltmacht	28
1.6	Box: So funktioniert das Solitaire-Verfahren	36
1.7	Deutsche Handverfahren im Zweiten Weltkrieg	38
1.8	Box: So funktionierten die deutschen Handverfahren	51
1.9	Das Buch, das keiner lesen kann	56
1.10	Die Jäger des verschlüsselten Schatzes	67
1.11	Box: Die Beale-Chiffren	75
1.12	Ungelöste Codes.....	79
1.13	Gelöste Codes.....	97
2	Das Zeitalter der Verschlüsselungsmaschinen	105
2.1	Verdrahtete Rotoren	105
2.2	Box: So funktionierte eine Rotormaschine	123
2.3	Die Enigma	124
2.4	Box: So funktionierte die Enigma	138
2.5	Box: Ein kleiner Enigma-Führer	139
2.6	Auf den Spuren der Kryha-Maschine.....	144
2.7	William Friedman knackt die Purple.....	155
2.8	Box: So funktionierte die Purple.....	162
2.9	Würmer aus Zahlen	165
2.10	Der Geheimschreiber	174
2.11	Box: So funktionierte der Geheimschreiber	183
2.12	Colossus gegen die Lorenz-Maschine.....	185
2.13	Box: So funktionierte die Lorenz-Maschine.....	196
2.14	Wie Boris Hagelin zum Millionär wurde	197
2.15	Box: So funktionierte eine C-Maschine von Hagelin	209
2.16	Windtalkers.....	211
2.17	Hitlers letzte Maschinen.....	217
2.18	Kryptophonie	228
2.19	Die unterschätzten deutschen Codeknacker.....	238
2.20	Verschlüsselung im Kalten Krieg	247
3	Das Zeitalter der Verschlüsselung mit dem Computer.	263
3.1	Der Data Encryption Standard	263
3.2	Box: So funktioniert der DES	273
3.3	Box: So funktioniert die vollständige Schlüsselsuche.....	274
3.4	Das öffentliche Geheimnis	275
3.5	Box: So funktioniert das Alice-Bob-Modell	286
3.6	Box: So funktioniert das Diffie-Hellman-Verfahren.....	286
3.7	Digitale Signaturen	287
3.8	Box: So funktioniert RSA	294
3.9	Sicherer als der Staat erlaubt: PGP.....	295
3.10	Kryptologie und Politik	303
3.11	Der Advanced Encryption Standard	309

3.12	Box: So funktioniert der AES	314
3.13	Hans Dobbertin knackt MD5	315
3.14	Der Cybermoney-Flop	321
3.15	Von Abrüstung bis Zero-Knowledge	329
3.16	Die Grundlagenkrise	339
3.17	Die brennende Generation	346
4	Zukunft und Fiktion der Verschlüsselung	353
4.1	Quanten und DNA.....	353
4.2	Kryptologie in Literatur und Film.....	358
5	Kryptologie in Museen	373
6	Die Software CrypTool	377
7	Rätsel der Kryptologie-Geschichte	379
8	Lösungen	381
9	Danksagung	389
10	Bildnachweis	391
Glossar	393	
Literatur	405	
Namens- und Organisationsindex	408	
Sachindex	411	