

Albrecht Beutelspacher

# **Kryptologie**

Albrecht Beutelspacher

# **Kryptologie**

Eine Einführung in die Wissenschaft vom  
Verschlüsseln, Verbergen und Verheimlichen.

Ohne alle Geheimniskrämerei,  
aber nicht ohne hinterlistigen Schalk,  
dargestellt zum Nutzen und Ergötzen  
des allgemeinen Publikums.

Fünfte, abermals leicht verbesserte Auflage

Springer Fachmedien Wiesbaden GmbH

Professor Dr. *Albrecht Beutelspacher*  
Fachbereich Mathematik der Universität Gießen

1. Auflage 1987
- 2., erweiterte und verbesserte Auflage 1991
- 3., verbesserte Auflage 1993
- 4., verbesserte Auflage 1994
- 5., verbesserte Auflage 1996

Alle Rechte vorbehalten

©Springer Fachmedien Wiesbaden, 1996

Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/  
Wiesbaden, 1996



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Gedruckt auf säurefreiem Papier

ISBN 978-3-528-48990-8

ISBN 978-3-663-10575-6 (eBook)

DOI 10.1007/978-3-663-10575-6

---

# Inhaltsverzeichnis

---

**Einleitung** 1

**Einige technische Hinweise** 8

**Kapitel 1 Caesar oder**

**Aller Anfang ist leicht!** 9

1.1 Die Skytale von Sparta 11

1.2 Verschiebechiffren 13

1.3 Monoalphabetische Chiffrierungen 20

1.4 Tauschchiffren 20

1.5 Schlüsselwörter 22

1.6 Kryptoanalyse 23

Übungsaufgaben 27

**Kapitel 2 Wörter und Würmer oder**

**Warum einfach, wenn's auch kompliziert geht?** 35

2.1 Verschleierung der Häufigkeiten 35

2.2 Die Vigenère-Chiffre 37

2.3 Kryptoanalyse 39

2.3.1 Der Kasiski-Test 40

2.3.2 Der Friedman-Test 43

2.3.3 Bestimmung des Schlüsselworts 49

2.4 Schlußbemerkungen 49

Übungsaufgaben 51

**Kapitel 3 Sicher ist sicher oder**

**Ein bißchen Theorie** 55

3.1 Chiffriersysteme 55

3.2 Perfekte Sicherheit 58

3.3 Das one-time Pad 63

3.4 Schieberegister 66

3.5 Kryptoanalyse von linearen Schieberegistern 71

Übungsaufgaben 75

|                  |  |            |
|------------------|--|------------|
| <b>Kapitel 4</b> | <b>Daten mit Denkkzettel oder<br/>Ein Wachhund namens Authentikation</b>   | <b>79</b>  |
| 4.1              | Motivation   | 79         |
| 4.2              | Integrität und Authentizität   | 82         |
| 4.2.1            | Mac'n Data   | 82         |
| 4.2.2            | Benutzerauthentikation   | 86         |
|                  | Paßwörter  | 87         |
|                  | Authentikation mit Chipkarten  | 90         |
| 4.2.3            | Zero-Knowledge-Protokolle  | 93         |
|                  | Historisches Beispiel: Das Geheimnis des Tartaglia                         | 94         |
|                  | Das Quadratwurzelspiel   | 95         |
|                  | Das Fiat-Shamir-Protokoll  | 97         |
| 4.3              | Chipkarten   | 100        |
| 4.3.1            | Chipkarten zur Zugangskontrolle  | 101        |
| 4.3.2            | Einkaufen mit der Karte  | 103        |
|                  | Übungsaufgaben   | 106        |
| <b>Kapitel 5</b> | <b>Die Zukunft hat schon begonnen oder<br/>Asymmetrische Kryptosysteme</b> | <b>113</b> |
| 5.1              | Asymmetrische Kryptosysteme  | 114        |
| 5.2              | Die elektronische Unterschrift   | 119        |
| 5.3              | Der RSA-Algorithmus  | 122        |
| 5.3.1            | Ein Satz von Euler   | 123        |
| 5.3.2            | Der euklidische Algorithmus  | 125        |
| 5.3.2.1          | Berechnung des ggT   | 125        |
| 5.3.2.2          | Berechnung der modularen Inversen  | 126        |
| 5.3.3            | Schlüsselerzeugung   | 128        |
| 5.3.4            | Wie benutzt man den RSA-Algorithmus?                                       | 129        |
| 5.3.5            | Die Stärke des RSA-Algorithmus   | 133        |
| 5.4              | Schlüsselaustausch   | 136        |
| 5.5              | Weitere Anwendungen des diskreten Logarithmus                              | 141        |
|                  | Übungsaufgaben   | 145        |

**Kapitel 6 Ach wie gut, daß niemand weiß, daß ich Rumpelstilzchen  
heiß oder**

**Wie bleibe ich anonym? 149**

**6.1 Was ist Anonymität? 149**

**6.2 Drei (zu) einfache Modelle 153**

**6.2.1 Anonymität des Empfängers. Broadcasting 153**

**6.2.2 Anonymität des Senders: Pseudonyme 153**

**6.2.3 Anonymität der Kommunikationsbeziehung:  
Rauschen 154**

**6.3 Elektronisches Geld 155**

**6.4 MIX as MIX can 159**

**Übungsaufgaben 164**

**Ausklang 167**

**Entschlüsselung der Geheimtexte 169**

**Literaturverzeichnis 171**

**Namen- und Sachverzeichnis 177**