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 **Polyalphabetische Chiffrierungen oder**
Warum einfach, wenn's auch kompliziert geht? 33
2.1 Verschleierung der Häufigkeiten 33
2.2 Die Vigenère-Chiffre 35
2.3 Kryptoanalyse 37
2.3.1 Der Kasiski-Test 38
2.3.2 Der Friedman-Test 41
2.3.3 Bestimmung des Schlüsselworts 47
2.4 Schlußbemerkungen 47
Übungsaufgaben 49

Kapitel 3 **Sicher ist sicher oder**
Ein bißchen Theorie 53
3.1 Chiffriersysteme 53
3.2 Perfekte Sicherheit 56
3.3 Das one-time Pad 61
3.4 Schieberegister 64
3.5 Kryptoanalyse von linearen Schieberegistern 69
Übungsaufgaben 73

Kapitel 4 Daten mit Denkzettel oder Ein Wachhund namens Authentikation 77
4.1 Motivation 77
4.2 Integrität und Authentizität 80
4.2.1 Mac 'n Data 80
4.2.2 Benutzerauthentifikation 84
Paßwörter 85
Authentikation mit Chipkarten 88
4.2.3 Zero-Knowledge-Protokolle 91
Historisches Beispiel: Das Geheimnis des Tartaglia 92
Das Quadratwurzelspiel 93
Das Fiat-Shamir-Protokoll 95
4.3 Chipkarten 98
4.3.1 Chipkarten zur Zugangskontrolle 99
4.3.2 Einkaufen mit der Karte 101
Übungsaufgaben 104

Kapitel 5 Die Zukunft hat schon begonnen oder Asymmetrische Kryptosysteme 111
5.1 Asymmetrische Kryptosysteme 112
5.2 Die elektronische Unterschrift 117
5.3 Der RSA-Algorithmus 120
5.3.1 Ein Satz von Euler 121
5.3.2 Der Euklidische Algorithmus 123
5.3.2.1 Berechnung des ggT 123
5.3.2.2 Berechnung der modularen Inversen 124
5.3.3 Schlüsselerzeugung 126
5.3.4 Wie benutzt man den RSA-Algorithmus? 127
5.3.5 Die Stärke des RSA-Algorithmus 131
5.4 Schlüsselaustausch 134
5.5 Weitere Anwendungen des diskreten Logarithmus 139
Übungsaufgaben 143

Kapitel 6 Ach wie gut, daß niemand weiß, daß ich Rumpelstilzchen heiß oder Wie bleibe ich anonym? 147
6.1 Was ist Anonymität? 147
6.2 Drei (zu) einfache Modelle 151
6.2.1 Anonymität des Empfängers. Broadcasting 151
6.2.2 Anonymität des Senders: Pseudonyme 151
6.2.3 Anonymität der Kommunikationsbeziehung: Rauschen 152
6.3 Elektronisches Geld 153
6.4 MIX as MIX can 157
Übungsaufgaben 162

Ausklang 165

Entschlüsselung der Geheimtexte 167

Literaturverzeichnis 169

Namen- und Sachverzeichnis 175