

# Inhaltsverzeichnis

<b>1</b>	<b>Cäsar oder Aller Anfang ist leicht!</b> .....	<b>1</b>
1.1	Die Skytala von Sparta .....	3
1.2	Verschiebechiffren .....	5
1.3	Kryptoanalyse .....	10
1.4	Monoalphabetische Chiffrierungen .....	14
1.5	Tauschchiffren .....	15
1.6	Schlüsselwörter .....	18
1.7	Kryptoanalyse .....	19
1.8	Moderne monoalphabetische Algorithmen .....	22
1.9	Übungsaufgaben .....	24
<b>2</b>	<b>Wörter und Würmer oder Warum einfach, wenn's auch kompliziert geht?</b> .....	<b>31</b>
2.1	Verschleierung der Häufigkeiten .....	32
2.2	Die Vigenère-Chiffre .....	33
2.3	Kryptoanalyse .....	36
2.3.1	Der Kasiski-Test .....	36
2.3.2	Der Friedman-Test .....	40
2.3.3	Bestimmung des Schlüsselworts .....	46
2.4	Schlussbemerkungen .....	47
2.5	Übungsaufgaben .....	48
<b>3</b>	<b>Sicher ist sicher oder Ein bisschen Theorie</b> .....	<b>53</b>
3.1	Chiffriersysteme .....	53
3.2	Perfekte Sicherheit .....	56
3.3	Das One-Time-Pad .....	60
3.4	Schieberegister .....	63
3.5	Kryptoanalyse von linearen Schieberegistern .....	67
3.6	Wie sicher ist Kryptographie? .....	72
3.7	Übungsaufgaben .....	73

<b>4</b>	<b>Daten mit Denkkzettel oder Ein Wachhund namens Authentifikation</b>	<b>77</b>
4.1	Motivation	77
4.2	Integrität und Authentizität	80
4.2.1	Mac 'n Data	80
4.2.2	Benutzerauthentifikation	84
4.2.3	Zero-Knowledge-Protokolle	92
4.3	Chipkarten	98
4.3.1	Chipkarten zur Zugangskontrolle	100
4.3.2	Einkaufen mit der Karte	102
4.4	Übungsaufgaben	104
<b>5</b>	<b>Die Zukunft hat schon begonnen oder Public-Key-Kryptographie</b>	<b>111</b>
5.1	Public-Key-Kryptosysteme	112
5.2	Die elektronische Signatur	117
5.3	Der RSA-Algorithmus	121
5.3.1	Ein Satz von Euler	122
5.3.2	Der euklidische Algorithmus	125
5.3.3	Schlüsselerzeugung	129
5.3.4	Anwendung des RSA-Algorithmus	131
5.3.5	Die Kunst zu potenzieren	135
5.3.6	Die Stärke des RSA-Algorithmus	136
5.4	Schlüsselaustausch	141
5.5	Weitere Anwendungen des diskreten Logarithmus	147
5.6	Die Authentizität der öffentlichen Schlüssel	150
5.7	Seitenkanalangriffe	152
5.8	Übungsaufgaben	153
<b>6</b>	<b>Ach wie gut, dass niemand weiß, dass ich Rumpelstilzchen heiß oder Wie bleibe ich anonym?</b>	<b>157</b>
6.1	Was ist Anonymität?	157
6.2	Drei (zu) einfache Modelle	161
6.2.1	Anonymität des Empfängers: Broadcasting	161
6.2.2	Anonymität des Senders: Pseudonyme	161
6.2.3	Anonymität der Kommunikationsbeziehung: Rauschen	162
6.3	Elektronisches Geld	162
6.4	MIX as MIX can	167
6.5	Übungsaufgaben	172

<b>Ausklang</b> .....	<b>173</b>
<b>Entschlüsselung der Geheimentexte</b> .....	<b>175</b>
<b>Anmerkungen zur Literatur</b> .....	<b>177</b>
<b>Literatur</b> .....	<b>179</b>
<b>Sachverzeichnis</b> .....	<b>185</b>