

# Inhalt

<b>I. Kryptographie: Geheimwissenschaft oder Wissenschaft von Geheimnissen? . . . . .</b>	<b>7</b>
<b>II. Ein erster Eindruck oder Einblicke in die Welt der klassischen Kryptographie . . . . .</b>	<b>14</b>
1. Verbergen der Existenz der Nachricht . . . . .	14
2. Verschlüsselung „ohne Schlüssel“ . . . . .	15
3. Was ist Kryptographie? . . . . .	18
4. Cäsar oder der Beginn der Kryptographie . . . . .	18
5. Was heißt „Verschlüsseln“? . . . . .	21
6. Kryptoanalyse des Cäsar-Codes . . . . .	23
7. Monoalphabetische Verschlüsselung . . . . .	25
8. Polyalphabetische Verschlüsselung . . . . .	29
9. Die Enigma . . . . .	33
10. Ziele der modernen Kryptographie . . . . .	36
<b>III. Wieviel Sicherheit gibt es? oder Wir gegen den Rest der Welt . . . . .</b>	<b>37</b>
1. Unknackbare Codes? . . . . .	37
2. Der DES . . . . .	41
3. Steht meine PIN verschlüsselt auf meiner ec-Karte? . . . . .	46
4. Schlüsselaustausch . . . . .	49
<b>IV. Public-Key-Kryptographie oder Allein gegen alle . . .</b>	<b>52</b>
1. Die Kunst, öffentlich geheime Süppchen zu kochen . . . . .	55
2. Natürliche Zahlen – zum ersten . . . . .	56
3. Der Diffie-Hellman-Schlüsselaustausch . . . . .	58
4. Der Trick mit den Briefkästen . . . . .	61
5. Natürliche Zahlen – zum zweiten . . . . .	64
6. Der RSA-Algorithmus . . . . .	67
7. Digitale Signaturen . . . . .	69

8. Hashfunktionen oder Small is beautiful . . . . .	70
9. PGP oder Anarchie ist machbar . . . . .	72
<b>V. Zero-Knowledge oder Ich weiß etwas, was Du</b>	
<b>nicht weißt. . . . .</b>	<b>77</b>
1. Der Wert eines Geheimnisses. . . . .	77
2. Das Geheimnis des Tartaglia . . . . .	79
3. Das Geheimnis der magischen Tür. . . . .	81
4. Natürliche Zahlen – zum dritten . . . . .	87
5. Das Fiat-Shamir-Verfahren . . . . .	91
<b>VI. Elektronisches Geld: ein Ding der Unmöglichkeit?</b>	<b>95</b>
1. Was ist Geld? . . . . .	95
2. Blinde Signatur . . . . .	101
3. Zwei Seiten der Medaille . . . . .	104
4. Resümee . . . . .	109
<b>VII. Wieviel Kryptographie braucht der Mensch? . . . . .</b>	<b>111</b>
1. Wieviel Kryptographie verträgt die Gesellschaft? . . . . .	111
2. Wie könnte man Einschränkungen der	
Kryptographie durchsetzen? . . . . .	118
3. Was nun? . . . . .	122
<b>Literatur . . . . .</b>	<b>124</b>
<b>Register . . . . .</b>	<b>125</b>