

Inhalt

I. Kryptographie: Geheimwissenschaft oder Wissenschaft von Geheimnissen?	7
II. Ein erster Eindruck oder Einblicke in die Welt der klassischen Kryptographie	14
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
III. Wie viel Sicherheit gibt es? oder Wir gegen den Rest der Welt	37
1. Unknackbare Codes?	37
2. Der DES	41
3. Steht meine PIN verschlüsselt auf meiner Bankkarte?	46
4. Schlüsselaustausch	49
IV. Public-Key-Kryptographie oder Allein gegen alle	52
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	70
8. Hashfunktionen oder Small is beautiful	71
9. PGP oder Anarchie ist machbar	73
V. Zero-Knowledge oder Ich weiß etwas, was du nicht weißt	78
1. Der Wert eines Geheimnisses	78
2. Das Geheimnis des Tartaglia	80
3. Das Geheimnis der magischen Tür	82
4. Natürliche Zahlen – zum Dritten	88
5. Das Fiat-Shamir-Verfahren	92
VI. Elektronisches Geld: ein Ding der Unmöglichkeit?	96
1. Was ist Geld?	96
2. Blinde Signatur	102
3. Resümee	105
4. Blockchain und Bitcoin	106
VII. Wie viel Kryptographie braucht der Mensch?	111
1. Wie viel Kryptographie verträgt die Gesellschaft? . .	111
2. Wie könnte man Einschränkungen der Kryptographie durchsetzen?	118
3. Was nun?	122
Literatur	124
Register	125