

Inhaltsverzeichnis

1 Grundlagen und Historisches	1
1.1 Worum es geht – das Szenario	1
1.2 Alphabete und Digitalisierung	3
1.3 Caesar-Chiffre	7
1.4 Geheimschrift der Illuminati	8
1.5 Vigenère-Chiffre	11
1.6 Kasiski- und Friedman-Angriff	14
1.7 Enigma-Maschine	16
2 Symmetrische Chiffren	21
2.1 Schlüssel und Angriffsstrategien	21
2.2 Vernam-Chiffre und Pseudozufall	24
2.3 GSM-Mobilfunk	27
2.4 Feistel-Chiffre	29
2.5 Data Encryption Standard DES	32
2.6 Betriebsmodi von Blockchiffren	41
2.7 UMTS-Mobilfunk und Digitalfernsehen	44
2.8 Advanced Encryption Standard AES	46
2.9 Festplatte und ZIP-Archiv	52
3 Public-Key-Chiffren	55
3.1 Faktorisierung und RSA-Chiffre	55
3.2 Internet und WLAN	61
3.3 Monte-Carlo-Primzahlen	64
3.4 Angriff durch Faktorisierung	68
3.5 Diskreter Logarithmus und Diffie-Hellman	72
3.6 Angriff mit Baby- und Giant-Steps	77
3.7 Bluetooth und ECDH	81
3.8 ElGamal-Chiffre	86
3.9 Knapsack und Merkle-Hellman-Chiffre	89

4	Digitale Signatur	91
4.1	Man-in-the-Middle-Angriff und Authentifikation	91
4.2	RSA- und ElGamal-Signatur	94
4.3	Hashwert und Secure Hash Algorithm SHA	99
4.4	E-Mail mit PGP und WhatsApp	105
4.5	DSA- und ECDSA-Signatur	108
4.6	Online-Banking	113
4.7	Blinde Signatur und Kryptowährungen	117
4.8	Passwortsicherheit und Challenge-Response	121
4.9	Handy, Kreditkarte und Reisepass	125
	Literatur	131
	Stichwortverzeichnis	137