

Inhalt

1	Elektronisches Bargeld, ein erstes Beispiel	15
2	Grundlagen	21
2.1	Terminologie	21
2.2	Kryptographische Algorithmen	22
2.3	Kryptographische Protokolle	24
2.4	Public-Key-Algorithmen	24
2.5	Kryptanalyse	26
2.6	Sicherheit von Schlüsseln	27
3	Klassische Chiffren	31
3.1	Verschiebechiffren	32
3.2	Multiplikative Chiffren	33
3.3	Tauschchiffren (Affine Chiffren)	35
3.4	Kryptanalyse monoalphabetischer Chiffren	36
3.5	Polyalphabetische Chiffren	37
3.5.1	Homophone Chiffren	37
3.6	Die Vigenère-Chiffre	38
3.6.1	Der Algorithmus	38
3.6.2	Kryptanalyse	40
3.6.3	Der Kasiski-Test	40
3.6.4	Der Friedman-Test	43
3.7	Die Enigma	45
3.7.1	Kryptanalyse	48
3.8	Das One-Time-Pad, die perfekte Chiffre	52
3.9	One-Time-Pad fast ohne Schlüsseltausch	55
3.10	Zusammenfassung	57

4	Moderne Blockchiffren	59
4.1	Data-Encryption-Standard DES	59
4.1.1	Übersicht	61
4.1.2	Eine Runde	63
4.1.3	Die 16 Teilschlüssel	64
4.1.4	Die Dechiffrierfunktion	64
4.1.5	Sicherheit und Nichtlinearität	66
4.1.6	Sicherheit und Geschwindigkeit	68
4.1.7	Triple-DES	68
4.2	Advanced-Encryption-Standard AES	68
4.2.1	Die Blockchiffre Rijndael	69
4.2.2	Die ByteSub-Transformation	70
4.2.3	Die ShiftRow-Transformation	71
4.2.4	Die MixColumn-Transformation	72
4.2.5	Die Schlüsselexpansion	72
4.2.6	Die inverse Chiffre	73
4.2.7	Geschwindigkeit	73
4.2.8	Sicherheit	73
4.2.9	Andere Funktionalitäten	74
4.3	Betriebsmodi von Blockchiffren	74
4.4	Andere Blockchiffren	75
5	Public-Key-Kryptographie	77
5.1	Merkles Rätsel	78
5.2	Der RSA-Algorithmus	79
5.2.1	Der Algorithmus	80
5.2.2	Sicherheit von RSA	82
5.2.3	Effiziente Primzahltests	83
5.2.4	Effizienz und Implementierung von RSA	84
5.2.5	Schnellere Implementierung von RSA	85
5.2.6	Angriffe gegen RSA	86
5.3	Angriffe gegen Public-Key-Verfahren	87
5.3.1	Chosen-Ciphertext-Angriff mit Social Engineering	87
5.3.2	Angriffe aufgrund von Seiteneffekten	87
5.3.3	Angriffe mit Spezialhardware	89
5.4	Schlüsseltausch	89
5.4.1	Schlüsseltausch mit symmetrischen Verfahren	89
5.4.2	Man-in-the-Middle-Angriff	90

5.4.3	Das Interlock-Protokoll.....	90
5.4.4	Schlüsseltausch mit Quantenkryptographie	91
5.5	Der Diffie-Hellman-Algorithmus	91
5.6	Der ElGamal-Algorithmus	93
5.7	Algorithmen mit Elliptischen Kurven	93
6	Authentifikation und digitale Signatur	97
6.1	Einwegfunktionen und Einweg-Hash-Funktionen.....	98
6.1.1	Passwortverschlüsselung.....	100
6.1.2	Der Geburtstagsangriff	100
6.2	Zero-Knowledge-Protokolle	102
6.2.1	Challenge-and-Response	102
6.2.2	Die Idee der Zero-Knowledge-Protokolle	103
6.2.3	Das Fiat-Shamir-Protokoll	104
6.3	Digitale Signaturen	105
6.3.1	Digital Signature Algorithm (DSA)	106
6.3.2	Blinde Signaturen	107
6.4	Digitale Signatur in der Praxis.....	108
6.4.1	Speichern des geheimen Schlüssels	108
6.4.2	Vertrauen in die Software	109
6.4.3	Zusammenfassung.....	110
6.5	Das Signaturgesetz.....	111
6.6	Authentifikation mit digitaler Signatur	112
6.7	Message-Authentication-Code (MAC)	113
6.8	Biometrische Verfahren	114
7	Public-Key-Infrastruktur	117
7.1	Persönliche Prüfung öffentlicher Schlüssel	117
7.2	Trustcenter.....	118
7.3	Zertifikatshierarchie	119
7.4	Web-of-Trust.....	120
7.5	Zukunft	121
8	Public-Key-Systeme	123
8.1	PGP	123
8.1.1	Schlüsseltausch mit PGP	126
8.1.2	Die Big-Brother-Funktion	126
8.1.3	GnuPG	127
8.1.4	Angriffe gegen PGP.....	128

8.2	S/MIME und das X.509-Protokoll.....	130
8.3	OpenPGP versus S/MIME	131
8.4	Secure shell (SSH).....	131
8.5	Secure socket layer (SSL).....	132
8.6	Virtual Private Networking und IP Security	133
8.7	Der neue Personalausweis.....	134
8.7.1	Hoheitliche Funktionen	134
8.7.2	Andere Funktionen	135
8.7.3	Digitale Signatur.....	135
8.7.4	Sicherheit des neuen Personalausweises	136
9	Elektronisches Bargeld	139
9.1	Secret-Splitting.....	139
9.2	Bit-Commitment-Protokolle	140
9.3	Protokolle für elektronisches Bargeld	141
10	Elektronische Zahlungssysteme	145
10.1	Die Geldkarte	146
10.2	Mondex.....	147
10.3	Ecash	148
10.4	Zahlung per Kreditkarte.....	148
10.4.1	Secure Electronic Transactions (SET)	148
10.4.2	PayPal	149
10.4.3	Andere Systeme.....	150
10.5	Zusammenfassung	150
11	Blockchain-Technologie und Bitcoin	151
11.1	Ein einführendes Beispiel.....	151
11.2	Vom virtuellen verteilten Kassenbuch zu Bitcoin	153
11.3	Authentizität der Nachricht	153
11.4	Berechnung des Kontostandes.....	154
11.5	Bestätigung der Zahlung durch die Mehrheit der Teilnehmer.....	154
11.6	Worin besteht das mathematische Rätsel?	155
11.7	Was sind die Eingabedaten in die Hash-Funktion?	156
11.8	Die Blockchain	156
11.9	Wie sieht ein Block bei Bitcoin aus?	158
11.10	Der Blockheader	158
11.11	Wie wird die Gültigkeit eines Blocks überprüft?	159
11.12	Die Arbeit eines Miners: Proof of Work (PoW)	159

11.13	Steuerung der Höhe des Schwellwertes	160
11.14	Das Rennen um die längste Kette.....	161
11.15	Die Geschichte von Bitcoin.....	161
11.16	Gibt es bei der Kryptowährung Bitcoin eine Inflation?	162
11.17	Ökologische Aspekte des Bitcoin-Systems (Stromverbrauch)	162
11.18	Public-Key-Infrastruktur versus Blockchain	164
12	Politische Randbedingungen	167
12.1	Starke Kryptographie und der Lauschangriff	167
12.2	US-Exportgesetze	169
13	Sicherheitslücken in der Praxis	171
Anhang		175
A	Arithmetik auf endlichen Mengen	175
A.1	Modulare Arithmetik	175
A.2	Invertierbarkeit in $\mathbb{Z}_n$	178
A.3	Der Euklidische Algorithmus.....	180
A.4	Die Eulersche φ -Funktion	183
A.5	Primzahlen.....	185
A.5.1	Primzahltests	186
A.6	Der endliche Körper $GF(2^8)$	190
A.6.1	Addition	190
A.6.2	Multiplikation.....	190
A.6.3	Polynome mit Koeffizienten in $GF(2^8)$	191
B	Erzeugen von Zufallszahlen	195
B.1	Pseudozufallszahlengeneratoren	197
B.1.1	Lineare Schieberegister mit Rückkopplung	198
B.1.2	Stromchiffren	200
B.2	Echte Zufallszahlen	201
B.2.1	Der Neumann-Filter	201
B.3	Zusammenfassung	203
C	Lösungen zu den Übungen	205
Literatur		227
Index		235