Inhaltsverzeichnis

1 Elektronisches Bargeld, ein erstes Beispiel **12**
1.1 Übungen 16

2 Grundlagen **17**
2.1 Terminologie 17
2.2 Kryptographische Algorithmen 18
2.3 Kryptographische Protokolle 21
2.4 Public-Key-Algorithmen 21
2.5 Kryptanalyse 23
2.6 Sicherheit von Schlüsseln 24
2.7 Übungen 26

3 Klassische Chiffren **28**
3.1 Verschiebechiffren 29
3.2 Multiplikative Chiffren 30
3.3 Tauschchiffren (Affine Chiffren) 31
3.4 Kryptanalyse monoalphabetischer Chiffren 33
3.5 Polyalphabetische Chiffren 34
3.6 Die Vigenère-Chiffre 35
3.7 Die Enigma 42
3.8 One-Time-Pad 47
3.9 One-Time-Pad fast ohne Schlüsseltausch 50
3.10 Zusammenfassung 52
3.11 Übungen 53

4 Moderne Blockchiffren **55**
4.1 Data-Encryption-Standard DES 55
4.2 Advanced-Encryption-Standard AES 65
4.3 Betriebsmodi von Blockchiffren 71
4.4 Andere Blockchiffren 72

4.5 Übungen 73

5 Public-Key-Kryptographie 75
5.1 Merkles Rätsel 76
5.2 Der RSA-Algorithmus 78
5.3 Angriffe gegen Public-Key-Verfahren 86
5.4 Schlüsseltausch 88
5.5 Der Diffie-Hellman-Algorithmus 91
5.6 Der ElGamal-Algorithmus 92
5.7 Algorithmen mit Elliptischen Kurven 93
5.8 Übungen 94

6 Authentifikation und digitale Signatur 96
6.1 Einwegfunktionen und Einweg-Hash-Funktionen 97
6.2 Zero-Knowledge-Protokolle 101
6.3 Digitale Signaturen 105
6.4 Digitale Signatur in der Praxis 107
6.5 Authentifikation mit digitaler Signatur 111
6.6 Message-Authentication-Code (MAC) 111
6.7 Biometrische Verfahren 112
6.8 Übungen 114

7 Public-Key-Infrastruktur 115
7.1 Persönliche Prüfung öffentlicher Schlüssel 115
7.2 Trustcenter 116
7.3 Zertifikatshierarchie 118
7.4 Web-of-Trust 119
7.5 Zukunft 119
7.6 Übungen 120

8 Public-Key-Systeme 121
8.1 PGP 122
8.2 S/MIME und das X.509 Protokoll 129
8.3 OpenPGP versus S/MIME 130
8.4 Secure shell (SSH) 130
8.5 Secure socket layer (SSL) 131
8.6 Virtual Private Networking und IP Security 132
8.7 Übungen 133

9 Elektronisches Bargeld 135
9.1 Secret-Splitting 136

9.2 Bit-Commitment-Protokolle 136
9.3 Protokolle für Elektronisches Bargeld 137
9.4 Übungen 139

10 Elektronische Zahlungssysteme 141
10.1 Die Geldkarte 142
10.2 Mondex 143
10.3 Ecash 144
10.4 Cybercash 145
10.5 Secure Electronic Transactions (SET) 145
10.6 Sonstige 146
10.7 Zusammenfassung 146

11 Politische Randbedingungen 148
11.1 Kryptographie und Lauschangriff 148
11.2 US-Exportgesetze 150
11.3 Signaturgesetz 151

12 Sicherheitslücken in der Praxis 154

Anhang 157

A Arithmetik auf endlichen Mengen 158
A.1 Modulare Arithmetik 158
A.2 Invertierbarkeit in $\mathbb{Z}_n$ 160
A.3 Der Euklidische Algorithmus 163
A.4 Die Eulersche φ-Funktion 165
A.5 Primzahlen 167
A.6 Der endliche Körper $GF(2^8)$ 172
A.7 Übungen 175

B Erzeugen von Zufallszahlen 177
B.1 Pseudozufallszahlengeneratoren 179
B.2 Echte Zufallszahlen 183
B.3 Zusammenfassung 185
B.4 Übungen 185

C Lösungen zu den Übungen 187

Literaturverzeichnis 209

Index 217