Inhaltsverzeichnis

1 Grundlagen **1**
- 1.1 Erste Grundbegriffe . . . 1
- 1.2 Kryptographische Systeme . . . 3
- 1.3 Informationstheoretische Grundlagen . . . 4
- 1.4 Komplexität von Berechnungen . . . 11

2 Klassische kryptographische Verfahren **13**
- 2.1 Transpositionschiffren . . . 13
- 2.2 Chiffren mit einfacher Substitution . . . 15
- 2.3 Chiffren mit homophoner Substitution . . . 19
- 2.4 Chiffren mit polyalphabetischer Substitution . . . 21
- 2.5 Chiffren mit Polygramm-Substitution . . . 30
- 2.6 Produktchiffren und Rotormaschinen . . . 32

3 Zahlentheoretische Grundlagen **35**
- 3.1 Modulare Arithmetik . . . 35
- 3.2 Bestimmung des modularen Inversen . . . 39
- 3.3 Lösen modularer Gleichungen . . . 45

4 Blockchiffren und ihre Betriebsarten **49**
- 4.1 Der DES . . . 49
- 4.2 IDEA . . . 57
- 4.3 Betriebsarten . . . 59

5 Exponentiationschiffren und das RSA-Public-Key-Kryptosystem **65**
- 5.1 Exponentiationschiffren . . . 65
- 5.2 Public-Key-Kryptosysteme . . . 67
- 5.3 Das RSA-Verfahren . . . 71
- 5.4 Erzeugung großer Primzahlen . . . 75
- 5.5 Sicherheitsüberlegungen für das RSA-Verfahren . . . 78

6 Hashfunktionen **87**
- 6.1 Hashfunktionen und Signaturen . . . 87
- 6.2 Kollisionsfreie Hashfunktionen . . . 89
- 6.3 Der Geburtstagsangriff . . . 91
- 6.4 Erweiterung von Hashfunktionen . . . 93
- 6.5 Hashfunktionen aus Kryptosystemen . . . 96
- 6.6 MD5 und SHA-1 . . . 97
- 6.7 Message Authentication Codes (MACs) . . . 101

Bibliografische Informationen
http://d-nb.info/989120937

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

7 Diskreter Logarithmus und kryptographische Anwendungen 105
7.1 Primitive Wurzeln und der diskrete Logarithmus 105
7.2 ElGamal-Public-Key-Verschlüsselungsverfahren 114
7.3 ElGamal-Public-Key-Signaturverfahren 119
7.4 Digital Signature Algorithm (DSA) 125
7.5 Zeitstempel bei Signaturverfahren 128
7.6 Eine weitere Hashfunktion 130

8 Schlüsselaustausch und Zertifikate 133
8.1 Schlüsselaustausch nach Diffie und Hellman 133
8.2 Vertrauenswürdige Instanzen und Zertifikate 135
8.3 Station-to-Station-Protokoll 141
8.4 MTI-Protokolle 143
8.5 Selbst-zertifizierende Schlüssel 145
8.6 Konferenzschlüssel 149
8.7 Quantenkryptographie 153

9 Quadratische Reste und das Rabin-Public-Key-Kryptosystem 157
9.1 Quadratische Reste 157
9.2 Quadratwurzeln 159
9.3 Rabin-Public-Key-Verschlüsselungsverfahren 164
9.4 Rabin-Public-Key-Signaturverfahren 167

10 Kryptographische Protokolle 169
10.1 Mentales Pokern 169
10.2 Vergessliche Übertragung 172
10.3 Protokoll zum Altersvergleich 183
10.4 Protokolle für Auktionen und Geschäfte 185
10.5 Elektronisches Geld (E-Cash) 189
10.6 Ein Protokoll für Wahlen 196

11 Zero-Knowledge-Protokolle 203
11.1 Einführung und Definitionen 203
11.2 Beweissystem für quadratische Reste 207
11.3 Beweissystem für diskrete Logarithmen 217
11.4 *NP*-Vollständigkeit 219
11.5 Zero-Knowledge-Protokolle für graphentheoretische Probleme 220

12 Der Advanced Encryption Standard 227
12.1 Mathematische Grundlagen 227
12.2 Bezeichnungen 230
12.3 Beschreibung der Chiffrierfunktion 232
12.4 Beschreibung der Dechiffrierfunktion 237

13 Kryptosysteme mit elliptischen Kurven 243
13.1 Elliptische Kurven 243
13.2 Kryptosysteme mit elliptischen Kurven 253

14 Identifikationsverfahren **257**
14.1 Einführung 257
14.2 Das Schnorr-Identifikationsverfahren 258
14.3 Das Okamoto-Identifikationsverfahren 264
14.4 Das Guillou-Quisquater-Identifikationsverfahren 268
14.5 Umwandlung von Identifikations- in Signaturverfahren 271

15 Secret-Sharing und gruppenorientierte Kryptographie **273**
15.1 Threshold-Secret-Sharing 274
15.2 Bedingt sicheres Schwellenwertverfahren 281
15.3 Nicht-interaktive Verifizierung von Shares 286
15.4 Schwellenwertverschlüsselung 291
15.5 Schwellenwertsignaturen 301

16 Kryptographie-Infrastruktur im Internet **307**
16.1 Pretty Good Privacy (PGP) 307
16.2 Signaturgesetz und Public-Key-Infrastruktur 311
16.3 SSL und IPSec 313
16.4 Key-Escrow-Systeme 316

Anhang: Häufigkeitstabellen **323**

Literaturverzeichnis **327**

Index **337**