

Inhaltsverzeichnis

| | |
|--|-----------|
| 1. Einleitung | 1 |
| 2. Ganze Zahlen | 3 |
| 2.1 Grundlagen | 3 |
| 2.2 Teilbarkeit | 4 |
| 2.3 Darstellung ganzer Zahlen | 5 |
| 2.4 O - und Ω -Notation | 7 |
| 2.5 Aufwand von Addition, Multiplikation und Division mit Rest | 7 |
| 2.6 Polynomzeit | 9 |
| 2.7 Größter gemeinsamer Teiler | 9 |
| 2.8 Euklidischer Algorithmus | 12 |
| 2.9 Erweiterter euklidischer Algorithmus | 15 |
| 2.10 Analyse des erweiterten euklidischen Algorithmus | 16 |
| 2.11 Zerlegung in Primzahlen | 20 |
| 2.12 Übungen | 22 |
| 3. Kongruenzen und Restklassenringe | 25 |
| 3.1 Kongruenzen | 25 |
| 3.2 Halbgruppen | 27 |
| 3.3 Gruppen | 29 |
| 3.4 Restklassenringe | 29 |
| 3.5 Körper | 30 |
| 3.6 Division im Restklassenring | 31 |
| 3.7 Rechenzeit für die Operationen im Restklassenring | 32 |
| 3.8 Prime Restklassengruppen | 33 |
| 3.9 Ordnung von Gruppenelementen | 34 |
| 3.10 Untergruppen | 36 |
| 3.11 Der kleine Satz von Fermat | 37 |
| 3.12 Schnelle Exponentiation | 38 |
| 3.13 Schnelle Auswertung von Potenzprodukten | 40 |
| 3.14 Berechnung von Elementordnungen | 41 |
| 3.15 Der Chinesische Restsatz | 43 |
| 3.16 Zerlegung des Restklassenrings | 45 |
| 3.17 Bestimmung der Eulerschen φ -Funktion | 46 |

| | | |
|-----------|--|-----------|
| 3.18 | Polynome | 47 |
| 3.19 | Polynome über Körpern | 49 |
| 3.20 | Konstruktion endlicher Körper | 51 |
| 3.21 | Struktur der Einheitengruppe endlicher Körper | 54 |
| 3.22 | Struktur der primen Restklassengruppe nach einer Primzahl .. | 55 |
| 3.23 | Übungen | 56 |
| 4. | Verschlüsselung | 59 |
| 4.1 | Verschlüsselungsverfahren | 59 |
| 4.2 | Private-Key-Verfahren und Public-Key-Verfahren | 60 |
| 4.3 | Sicherheit | 61 |
| 4.3.1 | Typen von Attacken | 61 |
| 4.3.2 | Randomisierte Verschlüsselung | 63 |
| 4.3.3 | Mathematische Modellierung | 64 |
| 4.4 | Alphabete und Wörter | 64 |
| 4.5 | Permutationen | 66 |
| 4.6 | Blockchiffren | 68 |
| 4.7 | Mehrfachverschlüsselung | 69 |
| 4.8 | Verschlüsselungsmodi | 69 |
| 4.8.1 | ECB-Mode | 69 |
| 4.8.2 | CBC-Mode | 71 |
| 4.8.3 | CFB-Mode | 74 |
| 4.8.4 | OFB-Mode | 76 |
| 4.9 | Stromchiffren | 77 |
| 4.10 | Die affine Chiffre | 79 |
| 4.11 | Matrizen und lineare Abbildungen | 80 |
| 4.11.1 | Matrizen über Ringen | 80 |
| 4.11.2 | Produkt von Matrizen mit Vektoren | 81 |
| 4.11.3 | Summe und Produkt von Matrizen | 81 |
| 4.11.4 | Der Matrizenring | 81 |
| 4.11.5 | Determinante | 82 |
| 4.11.6 | Inverse von Matrizen | 82 |
| 4.11.7 | Affin lineare Funktionen | 83 |
| 4.12 | Affin lineare Blockchiffren | 84 |
| 4.13 | Vigenère-, Hill- und Permutationschiffre | 85 |
| 4.14 | Kryptoanalyse affin linearer Blockchiffren | 85 |
| 4.15 | Sichere Blockchiffren | 87 |
| 4.15.1 | Konfusion und Diffusion | 87 |
| 4.15.2 | Exhaustive Key Search | 87 |
| 4.15.3 | Time-Memory Trade-Off | 88 |
| 4.15.4 | Differentielle Kryptoanalyse | 89 |
| 4.15.5 | Algebraische Kryptoanalyse | 90 |
| 4.16 | Übungen | 92 |

| | |
|--|-----|
| 5. Wahrscheinlichkeit und perfekte Geheimhaltung | 95 |
| 5.1 Wahrscheinlichkeit | 95 |
| 5.2 Bedingte Wahrscheinlichkeit | 96 |
| 5.3 Geburtstagsparadox | 98 |
| 5.4 Perfekte Geheimhaltung | 99 |
| 5.5 Das Vernam-One-Time-Pad | 101 |
| 5.6 Zufallszahlen | 102 |
| 5.7 Pseudozufallszahlen | 103 |
| 5.8 Übungen | 103 |
| 6. Der DES-Algorithmus | 105 |
| 6.1 Feistel-Chiffren | 105 |
| 6.2 Der DES-Algorithmus | 106 |
| 6.2.1 Klartext- und Schlüsselraum | 106 |
| 6.2.2 Die initiale Permutation | 107 |
| 6.2.3 Die interne Blockchiffre | 108 |
| 6.2.4 Die S-Boxen | 109 |
| 6.2.5 Die Rundenschlüssel | 109 |
| 6.2.6 Entschlüsselung | 111 |
| 6.3 Ein Beispiel für DES | 112 |
| 6.4 Sicherheit des DES | 113 |
| 6.5 Übungen | 114 |
| 7. Der AES-Algorithmus | 115 |
| 7.1 Bezeichnungen | 115 |
| 7.2 Cipher | 116 |
| 7.2.1 Identifikation der Bytes mit Elementen von $GF(2^8)$ | 117 |
| 7.2.2 SubBytes | 117 |
| 7.2.3 ShiftRows | 118 |
| 7.2.4 MixColumns | 119 |
| 7.2.5 AddRoundKey | 119 |
| 7.3 KeyExpansion | 120 |
| 7.4 Ein Beispiel | 121 |
| 7.5 InvCipher | 122 |
| 7.6 Übungen | 122 |
| 8. Primzahlerzeugung | 125 |
| 8.1 Probedivision | 125 |
| 8.2 Der Fermat-Test | 127 |
| 8.3 Carmichael-Zahlen | 127 |
| 8.4 Der Miller-Rabin-Test | 129 |
| 8.5 Zufällige Wahl von Primzahlen | 132 |
| 8.6 Übungen | 132 |

| | |
|--|-----|
| 9. Public-Key Verschlüsselung | 135 |
| 9.1 Idee | 135 |
| 9.2 Sicherheit | 136 |
| 9.2.1 Sicherheit des privaten Schlüssels | 137 |
| 9.2.2 Semantische Sicherheit | 137 |
| 9.2.3 Chosen-Ciphertext-Sicherheit | 138 |
| 9.2.4 Sicherheitsbeweise | 139 |
| 9.3 Das RSA-Verfahren | 139 |
| 9.3.1 Schlüsselerzeugung | 139 |
| 9.3.2 Verschlüsselung | 140 |
| 9.3.3 Entschlüsselung | 141 |
| 9.3.4 Sicherheit des geheimen Schlüssels | 142 |
| 9.3.5 RSA und Faktorisierung | 145 |
| 9.3.6 Auswahl von p und q | 145 |
| 9.3.7 Auswahl von e | 146 |
| 9.3.8 Auswahl von d | 147 |
| 9.3.9 Effizienz | 147 |
| 9.3.10 Multiplikativität | 148 |
| 9.3.11 Sichere Verwendung | 149 |
| 9.3.12 Verallgemeinerung | 150 |
| 9.4 Das Rabin-Verschlüsselungsverfahren | 151 |
| 9.4.1 Schlüsselerzeugung | 151 |
| 9.4.2 Verschlüsselung | 151 |
| 9.4.3 Entschlüsselung | 152 |
| 9.4.4 Effizienz | 153 |
| 9.4.5 Sicherheit gegen Ciphertext-Only-Attacks | 153 |
| 9.4.6 Eine Chosen-Ciphertext-Attacke | 154 |
| 9.4.7 Sichere Verwendung | 155 |
| 9.5 Diffie-Hellman-Schlüsselaustausch | 155 |
| 9.5.1 Diskrete Logarithmen | 155 |
| 9.5.2 Schlüsselaustausch | 156 |
| 9.5.3 Sicherheit | 157 |
| 9.5.4 Andere Gruppen | 158 |
| 9.6 Das ElGamal-Verschlüsselungsverfahren | 158 |
| 9.6.1 Schlüsselerzeugung | 158 |
| 9.6.2 Verschlüsselung | 159 |
| 9.6.3 Entschlüsselung | 159 |
| 9.6.4 Effizienz | 159 |
| 9.6.5 ElGamal und Diffie-Hellman | 160 |
| 9.6.6 Parameterwahl | 160 |
| 9.6.7 ElGamal ist randomisiert | 161 |
| 9.6.8 Verallgemeinerung | 161 |
| 9.7 Übungen | 162 |

| | |
|--|-----|
| 10. Faktorisierung | 165 |
| 10.1 Probedivision | 165 |
| 10.2 Die $p - 1$ -Methode | 166 |
| 10.3 Das Quadratische Sieb | 166 |
| 10.3.1 Das Prinzip | 167 |
| 10.3.2 Bestimmung von x und y | 167 |
| 10.3.3 Auswahl geeigneter Kongruenzen | 168 |
| 10.3.4 Das Sieb | 169 |
| 10.4 Analyse des Quadratischen Siebs | 171 |
| 10.5 Effizienz anderer Faktorisierungsverfahren | 173 |
| 10.6 Übungen | 174 |
| 11. Diskrete Logarithmen | 177 |
| 11.1 Das DL-Problem | 177 |
| 11.2 Enumeration | 178 |
| 11.3 Shanks Babystep-Giantstep-Algorithmus | 178 |
| 11.4 Der Pollard- ρ -Algorithmus | 180 |
| 11.5 Der Pohlig-Hellman-Algorithmus | 183 |
| 11.5.1 Reduktion auf Primzahlpotenzordnung | 184 |
| 11.5.2 Reduktion auf Primzahlordnung | 185 |
| 11.5.3 Gesamtalgorithmus und Analyse | 187 |
| 11.6 Index-Calculus | 187 |
| 11.6.1 Idee | 188 |
| 11.6.2 Diskrete Logarithmen der Faktorbasiselemente | 188 |
| 11.6.3 Individuelle Logarithmen | 190 |
| 11.6.4 Analyse | 190 |
| 11.7 Andere Algorithmen | 191 |
| 11.8 Verallgemeinerung des Index-Calculus-Verfahrens | 191 |
| 11.9 Übungen | 192 |
| 12. Kryptographische Hashfunktionen | 193 |
| 12.1 Hashfunktionen und Kompressionsfunktionen | 193 |
| 12.2 Geburtstagsattacke | 195 |
| 12.3 Kompressionsfunktionen aus Verschlüsselungsfunktionen | 196 |
| 12.4 Hashfunktionen aus Kompressionsfunktionen | 197 |
| 12.5 SHA-1 | 199 |
| 12.6 Andere Hashfunktionen | 201 |
| 12.7 Eine arithmetische Kompressionsfunktion | 201 |
| 12.8 Message Authentication Codes | 202 |
| 12.9 Übungen | 203 |

| | |
|--|-----|
| 13. Digitale Signaturen | 205 |
| 13.1 Idee | 205 |
| 13.2 Sicherheit | 206 |
| 13.2.1 Sicherheit des privaten Schlüssels | 206 |
| 13.2.2 No-Message-Modell | 206 |
| 13.2.3 Chosen-Message-Modell | 207 |
| 13.3 RSA-Signaturen | 207 |
| 13.3.1 Schlüsselerzeugung | 208 |
| 13.3.2 Erzeugung der Signatur | 208 |
| 13.3.3 Verifikation | 208 |
| 13.3.4 Angriffe | 209 |
| 13.3.5 Signatur von Texten mit Redundanz | 210 |
| 13.3.6 Signatur mit Hashwert | 211 |
| 13.3.7 Wahl von p und q | 211 |
| 13.3.8 Sichere Verwendung | 212 |
| 13.4 Signaturen aus Public-Key-Verfahren | 212 |
| 13.5 ElGamal-Signatur | 212 |
| 13.5.1 Schlüsselerzeugung | 213 |
| 13.5.2 Erzeugung der Signatur | 213 |
| 13.5.3 Verifikation | 213 |
| 13.5.4 Die Wahl von p | 214 |
| 13.5.5 Die Wahl von k | 215 |
| 13.5.6 Existentielle Fälschung | 215 |
| 13.5.7 Effizienz | 216 |
| 13.5.8 Sichere Verwendung | 217 |
| 13.5.9 Verallgemeinerung | 217 |
| 13.6 Der Digital Signature Algorithm (DSA) | 217 |
| 13.6.1 Schlüsselerzeugung | 217 |
| 13.6.2 Erzeugung der Signatur | 218 |
| 13.6.3 Verifikation | 218 |
| 13.6.4 Effizienz | 219 |
| 13.6.5 Sicherheit | 219 |
| 13.7 Das Lamport-Diffie Einmal-Signaturverfahren | 220 |
| 13.7.1 Schlüsselerzeugung | 221 |
| 13.7.2 Erzeugung der Signatur | 221 |
| 13.7.3 Verifikation | 221 |
| 13.7.4 Sicherheit | 222 |
| 13.8 Das Merkle-Verfahren | 223 |
| 13.8.1 Initialisierung | 224 |
| 13.8.2 Schlüsselerzeugung | 224 |
| 13.8.3 Erzeugung der Signatur | 225 |
| 13.8.4 Verifikation | 226 |
| 13.8.5 Sicherheit | 228 |
| 13.8.6 Verbesserungen | 229 |
| 13.9 Übungen | 230 |

| | |
|---|-----|
| 14. Andere Gruppen | 233 |
| 14.1 Endliche Körper | 233 |
| 14.2 Elliptische Kurven | 233 |
| 14.2.1 Definition | 234 |
| 14.2.2 Gruppenstruktur | 235 |
| 14.2.3 Kryptographisch sichere Kurven | 235 |
| 14.2.4 Vorteile von EC-Kryptographie | 236 |
| 14.3 Quadratische Formen | 237 |
| 14.4 Übungen | 237 |
| 15. Identifikation | 239 |
| 15.1 Anwendungen | 239 |
| 15.2 Paßwörter | 240 |
| 15.3 Einmal-Paßwörter | 241 |
| 15.4 Challenge-Response-Identifikation | 241 |
| 15.4.1 Verwendung von symmetrischer Kryptographie | 241 |
| 15.4.2 Verwendung von Public-Key-Kryptographie | 242 |
| 15.4.3 Zero-Knowledge-Beweise | 242 |
| 15.5 Übungen | 245 |
| 16. Secret Sharing | 247 |
| 16.1 Prinzip | 247 |
| 16.2 Das Shamir-Secret-Sharing-Protokoll | 247 |
| 16.2.1 Initialisierung | 248 |
| 16.2.2 Verteilung der Geheimnisteile | 248 |
| 16.2.3 Rekonstruktion des Geheimnisses | 249 |
| 16.2.4 Sicherheit | 250 |
| 16.3 Übungen | 250 |
| 17. Public-Key-Infrastrukturen | 251 |
| 17.1 Persönliche Sicherheitsumgebung | 251 |
| 17.1.1 Bedeutung | 251 |
| 17.1.2 Implementierung | 252 |
| 17.1.3 Darstellungsproblem | 252 |
| 17.2 Zertifizierungsstellen | 253 |
| 17.2.1 Registrierung | 253 |
| 17.2.2 Schlüsselerzeugung | 253 |
| 17.2.3 Zertifizierung | 254 |
| 17.2.4 Archivierung | 254 |
| 17.2.5 Personalisierung des PSE | 255 |
| 17.2.6 Verzeichnisdienst | 255 |
| 17.2.7 Schlüssel-Update | 256 |

XXIV Inhaltsverzeichnis

| | |
|--|------------|
| 17.2.8 Rückruf von Zertifikaten | 256 |
| 17.2.9 Zugriff auf ungültige Schlüssel | 256 |
| 17.3 Zertifikatsketten | 257 |
| Lösungen der Übungsaufgaben | 259 |
| Literaturverzeichnis | 271 |
| Sachverzeichnis | 275 |