

# Inhaltsverzeichnis

|          |  |            |
|----------|--|------------|
| <b>1</b> | <b>Von Geheimschriften zu Kryptosystemen</b>                           | <b>1</b>   |
| 1.1      | Geschichte und Grundbegriffe . . . . .                                 | 2          |
| 1.2      | Funktionen . . . . .   | 7          |
| 1.3      | Codierungen . . . . .  | 11         |
| 1.4      | Kryptosysteme . . . . .  | 15         |
| 1.5      | Zusammenfassung . . . . .  | 25         |
| <b>2</b> | <b>Die Suche nach Sicherheit und modulares Rechnen</b>                 | <b>29</b>  |
| 2.1      | Kryptoanalyse und der Begriff der Sicherheit . . . . .                 | 30         |
| 2.2      | Modulare Addition . . . . .  | 32         |
| 2.3      | Algebraische Strukturen . . . . .                                      | 38         |
| 2.4      | Modulare Multiplikation . . . . .                                      | 45         |
| 2.5      | Monoide . . . . .  | 46         |
| 2.6      | Gruppen . . . . .  | 50         |
| 2.7      | Verallgemeinerungen vom Kryptosystem CAESAR . . . . .                  | 54         |
| 2.8      | Zusammenfassung . . . . .  | 68         |
| <b>3</b> | <b>Entwurf und Kryptoanalyse von monoalphabetischen Kryptosystemen</b> | <b>73</b>  |
| 3.1      | Der Begriff der monoalphabetischen Kryptosysteme . . . . .             | 73         |
| 3.2      | Kryptoanalyse von monoalphabetischen Kryptosystemen . . . . .          | 76         |
| 3.3      | Verbesserung zu monoalphabetischen Kryptosystemen . . . . .            | 82         |
| 3.4      | Zusammenfassung . . . . .  | 88         |
| <b>4</b> | <b>Polyalphabetische Kryptosysteme und deren Kryptoanalyse</b>         | <b>93</b>  |
| 4.1      | Das polyalphabetische Kryptosystem VIGENÈRE . . . . .                  | 93         |
| 4.2      | Kryptoanalyse von VIGENÈRE . . . . .                                   | 98         |
| 4.3      | Statistische Kryptoanalyse von VIGENÈRE . . . . .                      | 104        |
| 4.4      | Der Euklidische Algorithmus . . . . .                                  | 122        |
| 4.5      | Homophone Kryptosysteme . . . . .                                      | 129        |
| 4.6      | Zusammenfassung . . . . .  | 132        |
| <b>5</b> | <b>Perfekte Sicherheit und das ONE-TIME-PAD-Kryptosystem</b>           | <b>137</b> |
| 5.1      | Die Entwicklung des ONE-TIME-PAD-Kryptosystems . . . . .               | 137        |
| 5.2      | Das mathematische Konzept der perfekten Sicherheit . . . . .           | 142        |

|           |  |            |
|-----------|--|------------|
| 5.3       | Sicherheitsgrad eines Kryptosystems . . . . .                                    | 152        |
| 5.4       | Zusammenfassung . . . . .  | 158        |
| <b>6</b>  | <b>Die ENIGMA und moderne Kryptosysteme</b>                                      | <b>163</b> |
| 6.1       | Die Geschichte der ENIGMA . . . . .  | 164        |
| 6.2       | Kryptographie im Zeitalter der Computer . . . . .                                | 174        |
| 6.3       | Moderne Kryptosysteme . . . . .  | 178        |
| 6.4       | Zusammenfassung . . . . .  | 181        |
| <b>7</b>  | <b>Der geheime Schlüsselaustausch und das DIFFIE-HELLMAN-Protokoll</b>           | <b>185</b> |
| 7.1       | Schlüsselaustausch mit einer verschließbaren Truhe . . . . .                     | 186        |
| 7.2       | Digitale Umsetzung des Schlüsselaustauschs . . . . .                             | 187        |
| 7.3       | Modulares Potenzieren und die schnelle Exponentiation . . . . .                  | 193        |
| 7.4       | Das DIFFIE-HELLMAN-Kommunikationsprotokoll . . . . .                             | 198        |
| 7.5       | Zusammenfassung . . . . .  | 204        |
| <b>8</b>  | <b>Komplexitätstheoretische Konzepte und eine neue Definition der Sicherheit</b> | <b>207</b> |
| 8.1       | Messung der Berechnungskomplexität von Algorithmen . . . . .                     | 210        |
| 8.2       | Vergleich der Effizienz unterschiedlicher Algorithmen . . . . .                  | 213        |
| 8.3       | Zeitkomplexität von algorithmischen Problemen . . . . .                          | 217        |
| 8.4       | Beispiele von schweren Problemen . . . . .                                       | 218        |
| 8.5       | Zusammenfassung . . . . .  | 232        |
| <b>9</b>  | <b>Das Konzept der Public-Key-Kryptographie</b>                                  | <b>237</b> |
| 9.1       | Das Public-Key-Kryptosystem DOMINATE . . . . .                                   | 244        |
| 9.2       | Das Untersummen-Problem als Grundlage für ein Public-Key-Kryptosystem . . . . .  | 259        |
| 9.3       | Ein Public-Key-Kryptosystem zum Verschicken eines Bits . . . . .                 | 276        |
| 9.4       | Zusammenfassung . . . . .  | 281        |
| <b>10</b> | <b>Zahlentheoretische Public-Key-Kryptosysteme und RSA</b>                       | <b>289</b> |
| 10.1      | Das Public-Key-Kryptosystem RABIN . . . . .                                      | 290        |
| 10.2      | Das Public-Key-Kryptosystem RSA . . . . .  | 318        |
| 10.3      | Zusammenfassung . . . . .  | 323        |
| <b>11</b> | <b>Anwendungen der Public-Key-Kryptographie und Kommunikationsprotokolle</b>     | <b>329</b> |
| 11.1      | Digitale Unterschrift von Dokumenten . . . . .                                   | 330        |
| 11.2      | Vergessliche Übertragung oder Münzwurf über das Telefon . . . . .                | 332        |
| 11.3      | Vergleich von zwei geheimen Zahlen . . . . .                                     | 337        |
| 11.4      | Zero-Knowledge-Beweissysteme . . . . .   | 340        |

|  |            |
|--|------------|
| 11.5 Teilen von Geheimnissen . . . . .     | 350        |
| 11.6 Zusammenfassung . . . . .             | 354        |
| <b>A Lösungen zu ausgewählten Aufgaben</b> | <b>359</b> |
| Lösungen zu Lektion 1 . . . . .            | 359        |
| Lösungen zu Lektion 2 . . . . .            | 361        |
| Lösungen zu Lektion 3 . . . . .            | 367        |
| Lösungen zu Lektion 4 . . . . .            | 369        |
| Lösungen zu Lektion 5 . . . . .            | 376        |
| Lösungen zu Lektion 6 . . . . .            | 378        |
| Lösungen zu Lektion 7 . . . . .            | 378        |
| Lösungen zu Lektion 8 . . . . .            | 380        |
| Lösungen zu Lektion 9 . . . . .            | 380        |
| Lösungen zu Lektion 10 . . . . .           | 387        |
| Lösungen zu Lektion 11 . . . . .           | 391        |
| <b>Literatur</b>                           | <b>393</b> |
| <b>Index</b>                               | <b>395</b> |