

# **Security**

Sommersemester 2022  
(LV 4120 und 7240)

## **Einleitung**

### **1. Einführung in die Informationssicherheit (70 Seiten)**

- 1.1 Begrifflichkeiten
  - 1.1.1 IT-Systeme
  - 1.1.2 Sicherheitsbegriffe
  - 1.1.3 Aktuelle Sicherheitslage
- 1.2 Daten, Nachrichten und Informationen
  - 1.2.1 Terminologie
  - 1.2.2 Nachrichten- und Informationsmodelle
  - 1.2.3 Kryptosysteme
- 1.3 Schutzziele der Datensicherheit
  - 1.3.1 Sicherheitsanforderungen und Sicherheitsziele
  - 1.3.2 Verschlüsselungsfunktionen und -algorithmen
  - 1.3.3 Kryptographische Hashfunktionen und digitale Signaturen
- 1.4 Basismechanismen der Kryptologie
  - 1.4.1 Ver- und Entschlüsselung
  - 1.4.2 Hashes und Message Authentication Code
  - 1.4.3 Digitale Signatur und Authentizität
- 1.5 Kryptanalyse
  - 1.5.1 Das Prinzip von Kerckhoffs
  - 1.5.2 Typen von Attacken
  - 1.5.3 Steganographie
- Zusammenfassung

## **2. Algebraische Strukturen und elementare Zahlentheorie (72 Seiten)**

- 2.1 Algebraische Strukturen und modulare Arithmetik
  - 2.1.1 Nomenklatur
  - 2.1.2 Algebraische Systeme
  - 2.1.3 Ganzzahlige Division mit Resten
  - 2.1.4 Kongruenzen und Teilbarkeit
  - 2.1.5 Euklidischer Algorithmus
  - 2.1.6 Sätze von Fermat und Euler
  - 2.1.7 Quadratische Reste und diskreter Logarithmus
  - 2.1.8 Einwegfunktionen und modulare Quadratwurzeln
- 2.2 Zahlentheorie und kryptologische Anwendungen
  - 2.2.1 Erweiterter Euklidischer Algorithmus
  - 2.2.2 Lösung Diophantischer Gleichungen
  - 2.2.3 Modulare Inversion
  - 2.2.4 Eulersche Phi-Funktion
  - 2.2.5 Entwicklungssatz
  - 2.2.6 Modulare Exponentiation
  - 2.2.7 Square-and-Multiply-Algorithmus
  - 2.2.8 Lösung simultaner Kongruenzen

Zusammenfassung

## **3. Monoalphabetische Chiffren und deren Analyse (24 Seiten)**

- 3.1 Einteilung der Chiffrierverfahren
  - 3.1.1 Transpositionschiffren
  - 3.1.2 Substitutionschiffren
- 3.2 Einfache Chiffriermaschinen
  - 3.2.1 Skytale
  - 3.2.2 Alberti-Scheibe
- 3.3 Komplexe Verschiebechiffren
  - 3.3.1 Multiplikative Chiffren
  - 3.3.2 Affine Tauschchiffren
- 3.4 Häufigkeitsanalyse
  - 3.4.1 Buchstabenverteilungen
  - 3.4.2 Bi- und Trigramme

Zusammenfassung

## **4. Symmetrische Verfahren und moderne Blockchiffren (82 Seiten)**

- 4.1 Symmetrische Blockverschlüsselung
  - 4.1.1 Schlüsselgesteuerte Transformation
  - 4.1.2 Gegenüberstellung
  - 4.1.3 Data Encryption Standard (DES)
  - 4.1.4 Advanced Encryption Standard (AES)
- 4.2 Betriebsmodi
  - 4.2.1 ECB
  - 4.2.2 CBC
  - 4.2.3 CFB
  - 4.2.4 OFB

- 4.3 Symmetrische Bitstromverschlüsselung
  - 4.3.1 XOR-Algorithmus
  - 4.3.2 One-Time-Pad und perfekte Sicherheit
- Zusammenfassung

## **5. Einwegfunktionen (25 Seiten)**

- 5.1 Einwegfunktionen und Hashfunktionen
  - 5.1.1 Integritätsschutz
  - 5.1.2 Hashfunktionen
- 5.2 Kryptographische Prüfsummen
  - 5.2.1 Message Digest (MD)
  - 5.2.2 Message Authentication Code (MAC)
- 5.3 Secure Hash Algorithm (SHA)
  - 5.3.1 Beschreibung des Verfahrens
  - 5.3.2 Praktische Implementierung
- Zusammenfassung

## **6. Asymmetrische Kryptosysteme (33 Seiten)**

- 6.1 ElGamal-Verschlüsselungsverfahren
  - 6.1.1 Algorithmus
  - 6.1.2 Zahlenbeispiel
- 6.2 Digitale Signaturen
  - 6.2.1 Ablaufskizze
  - 6.2.2 RSA-Signaturen
  - 6.2.3 Angriff auf RSA-Signatursysteme
- 6.3 Das Rabin-Verschlüsselungsverfahren
  - 6.3.1 Rabin-Modul und quadratische Reste
  - 6.3.2 Ver- und Entschlüsselung
  - 6.3.3 Sicherheit des Verfahrens
- 6.4 Signaturen und Authentifizierung
  - 6.4.1 ElGamal-Signaturen über  $\mathbb{Z}_p^*$
  - 6.4.2 Das Drei-Wege-Protokoll nach X.509
- Zusammenfassung

## **7. Schlüsselmanagement und Zufallszahlen (43 Seiten)**

- 7.1 Erzeugen von Zufallszahlen
  - 7.1.1 Zufallszahlengeneratoren
  - 7.1.2 Neumann-Filter
- 7.2 Pseudozufallszahlengeneratoren
  - 7.2.1 Lineare Schieberegister mit Rückkopplung
  - 7.2.2 Primzahlhäufigkeit und Primzahldichtefunktion
- 7.3 Primzahlen
  - 7.3.1 Zufallszahlen und lineare Kongruenzgeneratoren
  - 7.3.2 Primzahlen und Fundamentalsatz der Arithmetik
  - 7.3.3 Primzahlentests (Miller-Rabin-Test MRT)
  - 7.3.4 Rückgekoppelte Schieberegister
  - 7.3.5 Lineare Schieberegister mit Rückkopplung

- 7.4 Schlüsselmanagement
  - 7.4.1 Der Diffie-Hellman-Schlüsselaustausch (DH)
  - 7.4.2 Schlüsselhierarchie und Schlüsselklassen
- Zusammenfassung

## **8. Kryptographische Protokolle und Anwendungen (25 Seiten)**

- 8.1 Authentifikation und digitale Signatur
  - 8.1.1 Digitale Signaturen in der Praxis
  - 8.1.2 Authentifikation mit digitaler Signatur
- 8.2 Public-Key-Infrastruktur (PKI)
  - 8.2.1 Prüfung öffentlicher Schlüssel und Trustcenter
  - 8.2.2 Zertifikatshierarchie
- 8.3 Secret Sharing und Secret Splitting
  - 8.3.1 Secret Sharing
  - 8.3.2 Secret Splitting
- 8.4 Zero-Knowledge-Protokolle
  - 8.4.1 Challenge-and-Response-Verfahren
  - 8.4.2 Das Fiat-Shamir-Protokoll
- 8.5 Public-Key-Systeme
  - 8.5.1 PGP
  - 8.5.2 IPSec
- 8.6 Virtual Private Networking (VPN)
  - 8.6.1 Realisierung einer Übertragungssicherheit
  - 8.6.2 SSH und SSL
- Zusammenfassung

**Stand: 18.03.2022**