Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2021
(LV 4121 und 4241)

Einleitung

1. Einführung in die Informationssicherheit (64 Seiten)

2. Algebraische Strukturen und elementare Zahlentheorie (100 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
- 2.1.9 Modulare Quadratwurzel

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 Lösung simultaner Kongruenzen
- 2.2.8 Zufallszahlen und lineare Kongruenzgeneratoren
- 2.2.9 Primzahlen und Fundamentalsatz der Arithmetik
- 2.2.10 Primzahlentests
- 2.2.11 Rückgekoppelte Schieberegister
- 2.2.12 Bitstromverschlüsselung

Zusammenfassung

3. Monoalphabetische Chiffren und deren Analyse (24 Seiten)

3.1 Einteilung der Chiffrierverfahren
- 3.1.1 Transpostionschiffren
- 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. Moderne Blockchiffren und Schlüsselaustausch (84 Seiten)

4.1 Symmetrische Blockverschlüsselung
- 4.1.1 Schlüsselgesteuerte Transformation
- 4.1.2 Gegenüberstellung
- 4.1.3 Data Encryption Standard **DES**

Stand: 12.03.2021