

Kryptologie und Systemsicherheit (CS5303)

Inhaltsübersicht

SYMMETRISCHE CHIFFREN - Theorie und Anwendung

- Mathematische Grundlagen
- Monoalphabetische Chiffren und Grundbegriffe
- Polyalphabetische Chiffren
- Komposition von Verfahrensklassen
- Beispiel aus der Praxis: AES

GRUNDLEGENDE VERFAHREN UND PROTOKOLLE

- Mathematische Grundlagen und Begriffe
- Chipkarten
- Verschlüsselung mit öffentlichen Schlüsseln - RSA
- Schlüsseltausch und Schlüsselvereinbarung
- Integrität und Authentizität – MDC, MAC und digitale Signatur
- Beispiele aus der Praxis

SICHERHEITSKONTROLLE

- Grundbegriffe
- Benutzer- und Systembestimmte Zugriffskontrolle
- Rollenbasierte Zugriffskontrolle
- Firewalls
- Beispiele aus der Praxis

Die erfolgreiche Erarbeitung der in der Lehrveranstaltung behandelten Themen befähigt die Studierenden dazu in der beruflichen Praxis

- anspruchsvolle Aufgaben in den Bereichen Sicherheitsprojektierung und Sicherheitsmanagement wahrzunehmen und
- bei der Entwicklung von Sicherheitssystemen und -komponenten mitzuwirken.

Lehrbücher¹

- [BEUT05] A. BEUTELSPACHER U.A.: *Kryptografie in Theorie und Praxis - Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk*.
F. Vieweg, Braunschweig/Wiesbaden (2005).
- [BEUT07] A. BEUTELSPACHER: *Kryptologie*.
F. Vieweg, Braunschweig/Wiesbaden (2007).
- [BEUT04] A. BEUTELSPACHER, J. SCHWENK, K.-D. WOLFENSTETTER: *Moderne Verfahren der Kryptographie – Von RSA zu Zero Knowledge*
F. Vieweg, Braunschweig/Wiesbaden (2004).
- [ECKE07] C. ECKERT: *IT-Sicherheit*.
Oldenbourg, München/Wien (2007).
- [ERTE07] W. ERTEL: *Angewandte Kryptografie*.
Fachbuchverlag Leipzig im Carl Hanser Verlag, München/Wien (2007).
- [FUHR01] K. FUHRBERG U.A.: *Internet-Sicherheit*.
C. Hanser, München/Wien (2001).
- [SCHA03] G. SCHÄFER: *Netzicherheit*.
dpunkt.verlag, Heidelberg (2003).
- [STAL05] W. STALLINGS: *Cryptography and Network Security - Principles and Practice*.
Taylor & Francis Group (2005); ISBN-13: 978-1584885085
- [SCHN05] B. SCHNEIER: *Angewandte Kryptographie*.
Addison Wesley, Bonn/Reading Massachusetts u.a. (2005).

¹ Bei der hier empfohlenen Literatur handelt es um Grundlagenbücher. Sie decken oft mehr als die in der Vorlesung behandelten Lehrinhalte ab.