Kryptologie und Systemsicherheit (TI5006)

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

ZUGANGS- UND ZUGRIFFSKONTROLLE

- 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.

Lehrbücher[1]

[BEUT09] A. BEUTELSPACHER, H.B. NEUMANN, T. SCHWARPAUL: *Kryptografie in Theorie und Praxis - Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld*.
Vieweg+Teubner GWV Fachverlage GmbH, Wiesbaden (2009).
ISBN-13: 978-3834809773

[BEUT09] A. BEUTELSPACHER: *Kryptologie Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimniskrämerei, aber nicht ohne Nutzen und Ergötzen des allgemeinen Publikums*.
Vieweg+Teubner GWV Fachverlage GmbH, Wiesbaden (2009).
ISBN-13: 978-3834807038

[BEUT10] A. BEUTELSPACHER, J. SCHWENK, K.-D. WOLFENSTETTER: *Moderne Verfahren der Kryptographie – Von RSA zu Zero Knowledge*.
Vieweg+Teubner GWV Fachverlage GmbH, Wiesbaden (2010).
ISBN-13: 978-3834812285

[BUCH05] J. BUCHMANN: *Einführung in die Kryptographie*.
Springer-Lehrbuch, Heidelberg u.a. (2010). ISBN-13: 978-3642111853

[ECKE13] C. ECKERT: *IT-Sicherheit: Konzepte-Verfahren-Protokolle*.
Oldenbourg, München/Wien (2013). ISBN-13: 978-3486721386

[ERTE12] W. ERTEL: *Angewandte Kryptografie*.
Carl Hanser Verlag GmbH & Co. KG, München (2012).
ISBN-13: 978-3446427563

[STAL10] W. STALLINGS: *Cryptography and Network Security - Principles and Practice*.
Prentice Hall, Boston u.a. (2010). ISBN-13: 978-0136097044

[SCHN05] B. SCHNEIER: *Angewandte Kryptographie*.
Addison Wesley, Bonn/Reading Massachusetts u.a. (2005).
ISBN-13: 978-3827372284

[WÄTJ08] D. Wätjen: Kryptographie: Grundlagen, Algorithmen, Protokolle.
Spektrum Akademischer Verlag, Heidelberg (2008). ISBN-13: 978-3827419163

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