Modulnr.	**Modulname**	**Dozent(en)**
PTI893	Grundlagen der Informations-verarbeitung und -sicherheit	Prof. Dr. D. Lenk, Fak. PTI Prof. Dr. S. Schwarz, Fak. PTI

Studiengäng(e):

Informatik (B. Sc.)

Studienrichtung(-en)/-schwerpunkt(-e):

alle

Semester: 1. Semester (WS)

ECTS-Punkte: 6 **Arbeitsaufwand in h:** 180

Lehr- und Lernformen in h:

Vorlesung	60 (4 SWS)
Vor- und Nachbereitung	60
Selbststudium	60

Lernziele

Die Studierenden haben Kenntnisse von den mathematischen Grundlagen der Zahlenformate, der Informationstheorie und Codierungen. Sie kennen die wesentlichen Gefahren, denen IT-Systeme ausgesetzt sind und Möglichkeiten, diesen vorzubeugen.
Mathematische Grundlagen der Informatik: Die Studierenden beherrschen wichtige mathematische Grundlagen zur Darstellung der Zahlenformate sowie der Codierungsverfahren. Sie können technische Codierungen hinsichtlich ihrer Anwendung einschätzen. Bei Computerberechnungen auftretende Genauigkeitsprobleme werden aufgrund theoretischer Kenntnisse der Zahlensysteme richtig eingeordnet.
Informationssicherheit: Die Studierenden kennen informationstechnische Sicherheitsgefahren und können moderne kryptographische Verfahren der Verschlüsselung und digitalen Signaturen zum Schutz von Informationen anwenden.

Lehrinhalte

Mathematische Grundlagen der Informatik (Vorlesung: 30 h, Vor/Nachbereitung: 30 h, Selbststudium: 30 h)

- Grundlagen Informationstheorie, Elementarvorrat, Entscheidungsgehalt, Entropie, Redundanz
- Codierungen und ihre technisch-praktische Realisierung
- Ein- und mehrschrittige Codes
- Codesicherung, Fehlererkennende/ Fehlerkorrigierende Codes
- Geometrische Deutung des Coderaums, Stellendistanzen
- Codeoptimierung
- Zahlensysteme, Zahlendarstellung, Positionswertsysteme
- Konversion von Zahlen, Arithmetische Operationen, Negative Zahlendarstellungen
- Festkommadarstellung, Gleitkommadarstellung
- Genauigkeitsprobleme, Rundungsfehler

Informationssicherheit (Vorlesung: 30 h, Vor/Nachbereitung: 30 h, Selbststudium: 30 h)

- Grundlagen, Begriffe, Angriffsarten, Bedrohungen
- Verschlüsselung, Klassische Verfahren, Block- und Stromchiffren,
- Symmetrische Verschlüsselung, DES, AES, Schlüsselerzeugung, Betriebsmodi
- Asymmetrische Verschlüsselung, Schlüsselverteilungsproblem, RSA, Diffie-Hellman-Verfahren
- Hashfunktionen, MD5, SHA-1, MAC
- Digitale Signaturen, Zertifkate
- Pretty Good Privacy
- Schlüsselverwaltung, -vernichtung
- Authentifizierung, Klassen von Authentifikationsdiensten, Challenge-Response-Verfahren, Standard-Passwort-Verfahren, One-Time-Pad-Verfahren

Literatur

Mathematische Grundlagen der Informatik

- Blieberger , Burgstaller, Schildt: Informatik – Grundlagen, 4. Auflage 2001, Springer-Verlag
- Ernst: Grundkurs Informatik, 3. Auflage 2003, Vieweg-Verlag

Informationssicherheit

- Bruce Schneier: Angewandte Kryptographie, Pearson, 2005
- Eckert:IT-Sicherheit, Konzepte - Verfahren – Protokolle, Oldenbourg, 2006

- Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch, http://www.bsi.de/gshb/index.htm
- Steve Burnett, Stephen Paine: Kryptographie, mitp-Verlag, 2001

Voraussetzungen/Vorkenntnisse

keine

Leistungsnachweise

Art:	schriftliche Prüfungsleistung	**Zeitdauer:** 90 min
Vorleistungen:	keine	

Erarbeitet am: 17.01.09 durch: Prof. Schwarz, Prof. Lenk

PLS 04. Juni 2010