

Modul: Kryptologie 1

Lern- und Qualifikationsziele:

Inhalt: Dieses Modul bietet eine Einführung in grundlegende Verfahren der Kryptografie. Es werden sowohl klassische Verschlüsselungsverfahren (wie DES und AES) als auch Public-Key Systeme (wie RSA und ElGamal) behandelt. Die Benutzung von sicheren Verschlüsselungsverfahren bietet allerdings noch keine Garantie für einen sicheren Informationsaustausch. Hierzu bedarf es zusätzlich der Ausarbeitung sogenannter kryptografischer Protokolle, die den Ablauf aller Aktionen der verschiedenen Teilnehmer von der Schlüsselgenerierung über den Schlüsseltransport bis zur Ver- und Entschlüsselung der Nachrichten regeln.

Qualifikationsziele: Grundlegende Techniken beim Entwurf und der Analyse von Kryptosystemen und kryptografischen Protokollen.

Voraussetzungen für die Teilnahme am Modul:

Abschluss des Grundstudiums in Informatik.

Lehrveranstaltungen	SWS	SP und Beschreibung der Arbeitsleistung, auf deren Grundlage die SP vergeben werden
VL + UE	4 + 2	8 SP: Vorlesung (4 SWS) und Übungen (2SWS) aktive Teilnahme an den Übungen, Selbststudium
Voraussetzung für die Vergabe von Studienpunkten	Bei bestandener Prüfung am Ende des Semesters werden 8 Studienpunkte vergeben.	
Prüfung (Prüfungsform, Umfang/Dauer, SP)	Mündliche Prüfung	
Häufigkeit des Angebots	jedes zweite Wintersemester	
Dauer des Moduls	1 Semester	