

## Modul: Kryptologie 2

### Lern- und Qualifikationsziele:

Inhalt: Dieses Modul stellt eine Reihe von kryptografischen Methoden zum Erreichen wichtiger Schutzziele vor. Während im Modul Kryptologie 1 die Geheimhaltung von Nachrichten im Vordergrund stand, werden in diesem Modul kryptografische Protokolle zur Lösung folgender Aufgabenstellungen behandelt: Erstellung und Verifikation digitaler Signaturen, Authentikation von Nachrichten und Absender, Aufteilen einer Geheiminformation zwischen mehreren Parteien sowie die Durchführung von elektronischen Wahlen.

Qualifikationsziele: Fortgeschrittene Techniken beim Entwurf und der Analyse von kryptografischen Schutzmechanismen.

### Voraussetzungen für die Teilnahme am Modul:

Abschluss des Grundstudiums in Informatik sowie elementare Kenntnisse der Zahlentheorie wie sie beispielsweise im Modul Kryptologie 1 vermittelt werden.

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 Sommersemester	
Dauer des Moduls	1 Semester	