Modulbezeichnung	**Einführung in die Kryptographie**
Modulverantwortliche(r)	Prof. Dr. D. Hutter
Modulart	Pflicht/Wahl ☒ Wahlpflicht ☐
Spezialisierungsbereich	
Dauer des Moduls	1 Semester
Kreditpunkte	6 CP
Arbeitsaufwand	Berechnung des Workloads Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h
Turnus des Moduls	unregelmäßig
Voraussetzung für die Teilnahme	Keine ☐ Folgende: Inhaltliche Voraussetzungen: Programmierkenntnisse, Netzwerktechnik, Mathematische Grundlagen
Lehr- und Lernformen	Seminar ☐ Vorlesung ☒ Tutorium ☒ Praktikum ☐ Projekt ☐
Lernziele	• Grundlagen der Kryptographie und Kryptanalyse verstehen • Definitionen von kryptographischen Sicherheitskonzepten und Angreifer verstehen • Einsatz der Sicherheitsmechanismen und der elementaren Zahlentheorie in kryptographischen Systemen verstehen • Funktionsweisen und Einsatzgebiete der symmetrischen und asymmetrischen Kryptographie unterscheiden • Grundlegende und erweiterte Sicherheitsdienste der Kryptographie erlernen
Lerninhalte	• Grundbegriffe der Kryptographie und Kryptanalyse • Mathematische Grundlagen (modulare Arithmetik, endliche Körper) und elementare Zahlentheorie • Sicherheitsdefinitionen und Angreifermodelle • Historische Chiffren (Schiebe-, Substitution-, Vigenère-, etc.) • Blockchiffren (DES, AES) und Betriebsmodi • Message Authentication Codes • Kryptographische Hashfunktionen (SHA-1, SHA-3) • Trapdoor-Einwegfunktionen • Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung • RSA-Verfahren • Grundlagen Digitaler Signaturen • Elliptische Kurven Kryptographie (ECDH, ECIES, ECDSA) • Erweiterte Sicherheitsdienste (Commitment Schemes, Oblivious Transfer, Zero-Knowledge Proofs)
Prüfungsformen	Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

Literatur	• Christof Paar, Jan Pelzl: Understanding Crpytography, Springer-Verlag, 2010. Videomitschnitte unter www.crypto-textbook.com • Jonathan Katz,Yehuda Lindell, Introduction to Modern Cryptography, CRC PRESS, Boca Raton. • Nigel Smart, Cryptography Made Simple, Springer-Verlag