Einführung in die Kryptographie

Introduction to Cryptography

Modulnummer: MB-699.09

Master

Pflicht/Wahl	☐				
Wahl	☒	Basis	☒	Ergänzung	☐
Sonderfall	☐				

Zugeordnet zu Masterprofil

	Basis	Ergänzung
Sicherheit und Qualität (SQ)	☒	☐
KI, Kognition, Robotik (KIKR)	☐	☐
Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Mathematik und Theoretische Informatik

Modulteilbereich: 699 Spezielle Gebiete der Theoretischen Informatik

Anzahl der SWS

V	UE	K	S	Prak.	Proj.	Σ
2	2	0	0	0	0	4

Kreditpunkte: 6

Turnus: unregelmäßig

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: Programmierkenntnisse, Netzwerktechnik, Mathematische Grundlagen

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch/Englisch

Ziele:

- 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

Inhalte:

- 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)

Unterlagen (Skripte, Literatur, Programme usw.):

- 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

Form der Prüfung:
Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

Arbeitsaufwand	Präsenz	56 h
	Übungsbetrieb/Prüfungsvorbereitung	124 h
	Summe	180 h
Lehrende: Prof. Dr. D. Hutter, N.N.		Verantwortlich: Prof. Dr. D. Hutter