Modulbezeichnung			Kurzbezeichnung
Kryptographie und Datensicherheit			10-I=KD-102-m01
Modulverantwortung		**anbietende Einrichtung**	
Studiendekan/-in Informatik		Institut für Informatik	
ECTS	**Bewertungsart**	**zuvor bestandene Module**	
5	numerische Notenvergabe	--	
Moduldauer	**Niveau**	**weitere Voraussetzungen**	
1 Semester	weiterführend	Ggf. Vorleistungen wie vom Dozenten zu Veranstaltungsbeginn angekündigt (z.B. Lösen von Übungsaufgaben).	

Inhalte

Private-Key-Kryptosysteme, Vernam-One-Time-Pad, AES, perfekte Sicherheit, Public-Key-Kryptosysteme, RSA, Diffie-Hellman, Elgamal, Goldwasser-Micali, digitale Signatur, Challenge-Response-Verfahren, Secret Sharing, Millionärsproblem, Secure Circuit Evaluation, homomorphe Verschlüsselung.

Qualifikationsziele / Kompetenzen

Die Studierenden verfügen über grundlegende und anwendbare Kenntnisse auf den Gebieten Private-Key-Kryptosysteme, Vernam-One-Time-Pad, AES, perfekte Sicherheit, Public-Key-Kryptosysteme, RSA, Diffie-Hellman, Elgamal, Goldwasser-Micali, digitale Signatur, Challenge-Response-Verfahren, Secret Sharing, Millionärsproblem, Secure Circuit Evaluation, homomorphe Verschlüsselung.

Lehrveranstaltungen (Art, SWS, Sprache sofern nicht Deutsch)

V + Ü (keine Angaben zu SWS und Sprache verfügbar)

Erfolgsüberprüfung (Art, Umfang, Sprache sofern nicht Deutsch / Turnus sofern nicht semesterweise / Bonusfähigkeit sofern möglich)

Klausur (ca. 50-60 Min.). Kann nach Ankündigung des Dozenten bzw. der Dozentin vier Wochen vor dem Klausurtermin durch eine mündliche Einzel- oder Gruppenprüfung ersetzt werden (allein: 15 Min., zu zweit: 20 Min. zu dritt: 25 Min.).
Prüfungssprache: Deutsch, mit Einverständnis des/der Prüfenden auch Englisch

Platzvergabe

--

weitere Angaben

--

Arbeitsaufwand

--

Lehrturnus

--

Bezug zur LPO I

--

Verwendung des Moduls in Studienfächern

Master (1 Hauptfach) Informatik (2010)
Master (1 Hauptfach) Mathematik (2012)
Master (1 Hauptfach) Mathematik (2010)
Master (1 Hauptfach) Computational Mathematics (2012)
Erste Staatsprüfung für das Lehramt an Gymnasien Informatik (2009)