

Modulbezeichnung		Kurzbezeichnung
Kryptografie und Datensicherheit		10-I=KD-141-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	--
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. 60-120 Min.). Klausur kann nach Ankündigung des Dozenten bzw. der Dozentin zu Veranstaltungsbeginn durch eine mündliche Einzelprüfung (ca. 20 Min.) oder mündliche Gruppenprüfung (zu zweit ca. 30 Min.) ersetzt werden. Prüfungssprache: Deutsch, Englisch		
Platzvergabe		
--		
weitere Angaben		
--		
Bezug zur LPO I		
--		
Verwendung des Moduls in Studienfächern		
Master (1 Hauptfach) Informatik (2014)		