

Modulbezeichnung		Kurzbezeichnung
Kryptografie und Datensicherheit		10-I=KD-232-m01
Modulverantwortung		anbietende Einrichtung
Inhaber/-in des Lehrstuhls für Informatik I		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 (2) + Ü (2)		
Erfolgsüberprüfung (Art, Umfang, Sprache sofern nicht Deutsch / Turnus sofern nicht semesterweise / Bonusfähigkeit sofern möglich)		
Klausur (ca. 60-120 Min.) Klausur kann nach Ankündigung der Dozentin bzw. des Dozenten zu LV-Beginn durch eine mündliche Einzelprüfung (ca. 20 Min.) oder mündliche Gruppenprüfung (2 Teilnehmer, je ca. 15 Min.) ersetzt werden. Prüfungssprache: Deutsch und/oder Englisch Prüfungsturnus: im Semester der LV und im Folgesemester Bonusfähig		
Platzvergabe		
--		
weitere Angaben		
mögliche Schwerpunkte für den MA 120 Informatik: AT,SE,IT,KI,GE,SEC,IN		
Arbeitsaufwand		
150 h		
Lehrturnus		
k. A.		
Bezug zur LPO I		
--		
Verwendung des Moduls in Studienfächern		
Master (1 Hauptfach) Informatik (2023)		