Modulbezeichnung			Kurzbezeichnung
Kryptografie und Datensicherheit			10-I-KD-152-m01
Modulverantwortung		**anbietende Einrichtung**	
Studiendekan/-in Informatik		Institut für Informatik	
ECTS	**Bewertungsart**	**zuvor bestandene Module**	
5	numerische Notenvergabe	--	
Moduldauer	**Niveau**	**weitere Voraussetzungen**	
1 Semester	grundständig	--	

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 des Dozenten bzw. der Dozentin zu LV-Beginn durch eine mündliche Einzelprüfung (ca. 20 Min.) oder mündliche Gruppenprüfung (2 TN, ca. 15 Min. je TN) ersetzt werden.
Prüfungssprache: Deutsch und/oder Englisch
bonusfähig

Platzvergabe

--

weitere Angaben

--

Bezug zur LPO I

§ 22 II Nr. 3b

Verwendung des Moduls in Studienfächern

Bachelor (1 Hauptfach) Informatik (2015)
Bachelor (1 Hauptfach) Mathematik (2015)
Bachelor (1 Hauptfach) Computational Mathematics (2015)
Erste Staatsprüfung für das Lehramt an Gymnasien Informatik (2015)
LA Master Gymnasium MINT-Lehramt PLUS im Elitenetzwerk Bayern (ENB) (2016)
Zusatzstudium MINT-Lehramt PLUS im Elitenetzwerk Bayern (ENB) (2016)
Bachelor (1 Hauptfach) Informatik (2017)