

Modulbezeichnung		Kurzbezeichnung
Mathematische Aspekte der modernen Kryptographie		10-M-KRY-232-m01
Modulverantwortung		 anbietende Einrichtung
Studiendekan/-in Mathematik		Institut für Mathematik
ECTS	Bewertungsart	zuvor bestandene Module
5	bestanden / nicht bestanden	--
Moduldauer	Niveau	weitere Voraussetzungen
1 Semester	grundständig	--
Inhalte		
Grundlagen der elementaren Zahlentheorie, Public-Key-Kryptographie, Rechnen mit Quantencomputern, der Faktorisierungsalgorithmus von Shor, Postquantum-Kryptographie.		
Qualifikationsziele / Kompetenzen		
Der/die Studierende kennt die wesentlichen Methoden und Grundbegriffe der elementaren Zahlentheorie, ihre Anwendung in Public-Key-Kryptosystemen, und Rechenverfahren und Algorithmen von Quantencomputern.		
Lehrveranstaltungen (Art, SWS, Sprache sofern nicht Deutsch)		
V (3) + Ü (1)		
Erfolgsüberprüfung (Art, Umfang, Sprache sofern nicht Deutsch / Turnus sofern nicht semesterweise / Bonusfähigkeit sofern möglich)		
a) Klausur (ca. 60-120 Min., Regelfall) oder b) Mündliche Einzelprüfung (15-30 Min.) oder c) Mündliche Gruppenprüfung (2 TN, je 10-15 Min.) Prüfungssprache: Deutsch und/oder Englisch Prüfungsturnus: Im Semester der LV und im Folgesemester bonusfähig		
Platzvergabe		
--		
weitere Angaben		
--		
Arbeitsaufwand		
150 h		
Lehrturnus		
k. A.		
Bezug zur LPO I		
--		
Verwendung des Moduls in Studienfächern		
Exchange Austauschprogramm Mathematik (2023) Erste Staatsprüfung für das Lehramt an Gymnasien Mathematik (2023) Bachelor (1 Hauptfach) Mathematik (2023) Bachelor (1 Hauptfach) Mathematische Physik (2024)		