Modultitel	Modulcode
Kryptographie	math-Krypto-m
Modulverantwortliche(r)	
Dr. rer. nat. Barbara Maria Langfeld	
Veranstalter	
Sektion Mathematik	
Fakultät	
Mathematisch-Naturwissenschaftliche Fakultät	
Prüfungsamt	
Prüfungsamt Mathematik	

Leistungspunkte	9
Bewertung	Benotet
Dauer	ein Semester
Angebotshäufigkeit	Findet unregelmäßig statt
Arbeitsaufwand pro Leistungspunkt	30 Stunden
Arbeitsaufwand insgesamt	270 Stunden
Präsenzstudium	84 Stunden
Selbststudium	186 Stunden
Lehrsprache	Deutsch

Empfohlene Voraussetzung			
Lineare Algebra I + II; Algebra I			
Modulveranstaltung(en)			
Veranstaltungsart	**Lehrveranstaltungstitel**	**Pflicht/Wahl**	**SWS**
Vorlesung	Kryptographie	Wahl	4
Übung	Kryptographie	Wahl	2
Voraussetzungen für die Zulassung zu der/den Prüfung(en) (Vorleistungen)			
Aktive, regelmäßige Übungsteilnahme			

Prüfung(en)				
Prüfungstitel	**Prüfungsform**	**Bewertung**	**Pflicht/Wahl**	**Gewicht**
Modulprüfung: Kryptographie	Modulprüfung	Benotet	Pflicht	-

Lehrinhalte
Symmetrische Kryptosysteme; Public-key-verfahren; Beispiele von Falltürfunktionen, Faktorisierungsprobleme, Rechnen in endlichen Körpern, Diffie-Hellman-Schlüsseltausch, Massey-Omura-System, quadratisches Reziprozitätsgesetz, Quadratic-Residue-Cipher-System, RSA-Verfahren, El Gamal-System,DAS-Verfahren, elektronische Unterschrift, Primzahltests, elliptischen Kurven (über Ringen) und ECMMethode, Pollard-Methode; eventuell Grundbegriffe der Codierungstheorie.
Lernziele
Erwerb von Kenntnissen asymmetrischer Kryptosysteme und der algebraischen Hilfsmittel, eventuell mit Einführung in die Codierungstheorie
Literatur
Vorlesungsskript, Handbook of Applied Cryptography; Menezes, Alfred J. / van Oorschot, Paul C. / Vanstone, Scott A., CRC-Press 1997;
Weitere Angaben
Reine Mathematik

Verwendung	**Pflicht/Wahl**	**Fachsemester**
Bachelor, 1-Fach, Mathematik, (Version 2007)	Wahl	-
Erweiterungsfach auf der Masterebene, Mathematik, (Version 2007)	Wahl	-
Master, 1-Fach, Finanzmathematik, (Version 2007)	Wahl	-
Master, 1-Fach, Mathematik, (Version 2007)	Wahl	-
Master, 2-Fächer, Profil Handelslehrer, Mathematik, (Version 2007)	Wahl	-
Master, 2-Fächer, Profil Lehramt an Gymnasien, Mathematik, (Version 2007)	Wahl	-