Modulbezeichnung	**Kryptographie und Zahlentheorie (deleted:Tue Jul 17 08:42:15 +0200 2012)**
Modulverantwortliche(r)	Studiendekan Mathemathik
Modulart	Pflicht/Wahl ☒ Wahlpflicht ☐
Spezialisierungsbereich	
Dauer des Moduls	1 Semester
Kreditpunkte	9 CP
Arbeitsaufwand	Berechnung des Workloads Präsenz 84 h Übungsbetrieb/Prüfungsvorbereitung 186 h Summe 270 h
Turnus des Moduls	i.d.R. unregelmäßig angeboten
Voraussetzung für die Teilnahme	Keine ☒ Folgende
Lehr- und Lernformen	Seminar ☐ Vorlesung ☒ Tutorium ☒ Praktikum ☐ Projekt ☐
Lernziele	• Grundlegende Begriffe, Methoden und algorithmische Techniken der Zahlentheorie • Einsatz von Computer-Algebra-Systemen • Theoretisches und praktisches Verständnis moderner zahlentheoretischer Methoden für Verschlüsselung und Digitale Signatur
Lerninhalte	• Kongruenzen • Primfaktorzerlegung, Primzahltests • Euklidische Ringe, endliche Körper • Quadratische Reziprozität • Public Key Kryptographie mit RSA und diskretem Logarithmus • Elliptische Kurven und ihre Anwendung in der Kryptographie
Prüfungsformen	Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung.
Literatur	• N. Koblitz. A Course in Number Theory and Cryptography, Springer, 1994. • O. Forster. Algorithmische Zahlentheorie, Vieweg, 1996. • J. Buchmann. Einführung in die Kryptographie, Springer, 2003. • A. Werner. Elliptische Kurven in der Kryptographie, Springer, 2002