

Kryptographie und Zahlentheorie (deleted:Tue Jul 17 08:42:15 +0200 2012)							Modulnummer:		
<i>Cryptography and Number Theory</i>									
Bachelor Pflicht/Wahl <input checked="" type="checkbox"/> Wahlpflicht <input type="checkbox"/> Wahl <input type="checkbox"/> Sonderfall <input type="checkbox"/>				Modulbereich: Kein Schwerpunkt					
Anzahl der SWS	V	UE	K	S	Prak.	Proj.	Σ	Kreditpunkte: 9	Turnus i.d.R. unregelmäßig angeboten
	4	2	0	0	0	0	6		
Formale Voraussetzungen: -									
Inhaltliche Voraussetzungen: -									
Vorgesehenes Semester: ab 1. Semester									
Sprache: Deutsch									
Ziele: <ul style="list-style-type: none"> • 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 									
Inhalte: <ul style="list-style-type: none"> • 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 									
Unterlagen (Skripte, Literatur, Programme usw.): <ul style="list-style-type: none"> • 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 									
Form der Prüfung: Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung.									
Arbeitsaufwand		Präsenz		84 h		Übungsbetrieb/Prüfungsvorbereitung		186 h	
		Summe		270 h					
Lehrende: Angeboten durch Studiengang Mathematik, Durchführung wechselnd							Verantwortlich: Studiendekan Mathematik		