

Kryptographie und Zahlentheorie (deleted:Tue Jul 17 08:42:15 +0200 2012) <i>Cryptography and Number Theory</i>		Modulnummer: ME-600.04															
Master Pflicht/Wahl <input type="checkbox"/> Wahl <input checked="" type="checkbox"/> Basis <input type="checkbox"/> Ergänzung <input checked="" type="checkbox"/> Sonderfall <input type="checkbox"/>		Zugeordnet zu Masterprofil Basis Ergänzung Sicherheit und Qualität (SQ) <input type="checkbox"/> <input checked="" type="checkbox"/> KI, Kognition, Robotik (KIKR) <input type="checkbox"/> <input type="checkbox"/> Digitale Medien und Interaktion (DMI) <input type="checkbox"/> <input type="checkbox"/>															
Modulbereich: Mathematik und Theoretische Informatik Modulteilbereich: 600 Mathematik																	
Anzahl der SWS	<table border="1"> <tr><td>V</td><td>UE</td><td>K</td><td>S</td><td>Prak.</td><td>Proj.</td><td>Σ</td></tr> <tr><td>4</td><td>2</td><td>0</td><td>0</td><td>0</td><td>0</td><td>6</td></tr> </table>	V	UE	K	S	Prak.	Proj.	Σ	4	2	0	0	0	0	6	Kreditpunkte: 9	Turnus i.d.R. unregelmäßig angeboten
V	UE	K	S	Prak.	Proj.	Σ											
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	<table border="1"> <tr><td>Präsenz</td><td>84 h</td></tr> <tr><td>Übungsbetrieb/Prüfungsvorbereitung</td><td>186 h</td></tr> <tr><td>Summe</td><td>270 h</td></tr> </table>	Präsenz	84 h	Übungsbetrieb/Prüfungsvorbereitung	186 h	Summe	270 h										
Präsenz	84 h																
Übungsbetrieb/Prüfungsvorbereitung	186 h																
Summe	270 h																
Lehrende: Angeboten durch Studiengang Mathematik, Durchführung wechselnd		Verantwortlich: Studiendekan Mathematik															