

Modulbezeichnung	<b>Kryptographie und Zahlentheorie (deleted:Tue Jul 17 08:42:15 +0200 2012)</b>								
Modulverantwortliche(r)	Studiendekan Mathematik								
Modulart	Pflicht/Wahl <input checked="" type="checkbox"/> Wahlpflicht <input type="checkbox"/>								
Spezialisierungsbereich									
Dauer des Moduls	1 Semester								
Kreditpunkte	9 CP								
Arbeitsaufwand	<table style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">Berechnung des Workloads</td> </tr> <tr> <td style="padding-right: 20px;">Präsenz</td> <td style="text-align: right;">84 h</td> </tr> <tr> <td style="padding-right: 20px;">Übungsbetrieb/Prüfungsvorbereitung</td> <td style="text-align: right;">186 h</td> </tr> <tr> <td style="padding-right: 20px;">Summe</td> <td style="text-align: right; border-top: 1px solid black;">270 h</td> </tr> </table>	Berechnung des Workloads		Präsenz	84 h	Übungsbetrieb/Prüfungsvorbereitung	186 h	Summe	270 h
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 <input checked="" type="checkbox"/> Folgende								
Lehr- und Lernformen	Seminar <input type="checkbox"/> Vorlesung <input checked="" type="checkbox"/> Tutorium <input checked="" type="checkbox"/> Praktikum <input type="checkbox"/> Projekt <input type="checkbox"/>								
Lernziele	<ul style="list-style-type: none"> <li>• Grundlegende Begriffe, Methoden und algorithmische Techniken der Zahlentheorie</li> <li>• Einsatz von Computer-Algebra-Systemen</li> <li>• Theoretisches und praktisches Verständnis moderner zahlentheoretischer Methoden für Verschlüsselung und Digitale Signatur</li> </ul>								
Lerninhalte	<ul style="list-style-type: none"> <li>• Kongruenzen</li> <li>• Primfaktorzerlegung, Primzahltests</li> <li>• Euklidische Ringe, endliche Körper</li> <li>• Quadratische Reziprozität</li> <li>• Public Key Kryptographie mit RSA und diskretem Logarithmus</li> <li>• Elliptische Kurven und ihre Anwendung in der Kryptographie</li> </ul>								
Prüfungsformen	Erfolgreiche Bearbeitung der Übungsaufgaben, mündliche Prüfung.								
Literatur	<ul style="list-style-type: none"> <li>• N. Koblitz. A Course in Number Theory and Cryptography, Springer, 1994.</li> <li>• O. Forster. Algorithmische Zahlentheorie, Vieweg, 1996.</li> <li>• J. Buchmann. Einführung in die Kryptographie, Springer, 2003.</li> <li>• A. Werner. Elliptische Kurven in der Kryptographie, Springer, 2002</li> </ul>								