Kryptographie und Zahlentheorie (deleted:Tue Jul 17 08:42:15 +0200 2012)

Cryptography and Number Theory

Modulnummer: ME-600.04

Master

Pflicht/Wahl	☐				
Wahl	☒	Basis	☐	Ergänzung	☒
Sonderfall	☐				

Zugeordnet zu Masterprofil

	Basis	Ergänzung
Sicherheit und Qualität (SQ)	☐	☒
KI, Kognition, Robotik (KIKR)	☐	☐
Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Mathematik und Theoretische Informatik

Modulteilbereich: 600 Mathematik

Anzahl der SWS

V	UE	K	S	Prak.	Proj.	Σ
4	2	0	0	0	0	6

Kreditpunkte: 9

Turnus: i.d.R. unregelmäßig angeboten

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: -

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch

Ziele:

- 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:

- 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.):

- 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 Mathemathik