Anlage 2: Modulbeschreibung zum Diplomstudiengang Mathematik

Vertiefungsmodul

Modulnummer	M10
Modulname	Kryptologie/Datensicherheit
Modulverantwortlich	Studiendekan der Fakultät für Mathematik
Inhalte und Qualifikationsziele	Inhalte: • Begriff der Sicherheit von Information • Klassische Verschlüsselungsverfahren (Caesar-, Vigenere-, Hill-Chiffre u.a.) • Prinzipielle Verschlüsselungsmethoden (Substitutionschiffren, Transpositionschiffren) • Angriffsarten, Kryptoanalytische Methoden (Verteilungen, Kassiski-Methode, u.a.) • Moderne symmetrische Verschlüsselungsverfahren, Public Key Kryptosysteme, Digitale Unterschriften und Angriffe Qualifikationsziele: Ziel dieses angewandten Moduls ist die Einführung in kryptographische und kryptoanalytische Methoden (sowohl klassische als auch moderne). Insbesondere werden Verschlüsselungsverfahren sowie Methoden zum Brechen der Verschlüsselung behandelt. Aus diesem Wissen ergibt sich die Kompetenz, für spezielle Anwendungsgebiete jeweils geeignete Verschlüsselungsverfahren und Authentifikationsprotokolle einzusetzen.
Lehrformen	Lehrformen des Moduls sind Vorlesung und Übung. • V: Kryptologie/Datensicherheit (2 LVS) • Ü: Kryptologie/Datensicherheit (2 LVS)
Voraussetzungen für die Teilnahme (empfohlene Kenntnisse und Fähigkeiten)	keine
Verwendbarkeit des Moduls	---
Voraussetzungen für die Vergabe von Leistungspunkten	Die Erfüllung der Zulassungsvoraussetzung für die Prüfungsleistung und die erfolgreiche Ablegung der Modulprüfung sind Voraussetzungen für die Vergabe von Leistungspunkten. Zulassungsvoraussetzung ist folgende Prüfungsvorleistung (unbegrenzt wiederholbar): • Nachweis von 4 bis 14 Übungsaufgaben zu Kryptologie/Datensicherheit. Der Nachweis ist erbracht, wenn mindestens 40 % der geforderten Aufgaben richtig gelöst worden sind.
Modulprüfung	Die Modulprüfung besteht aus einer Prüfungsleistung: • 90-minütige Klausur zum Inhalt des Moduls (Prüfungsnummer: 20037)
Leistungspunkte und Noten	In dem Modul werden 4 Leistungspunkte erworben. Die Bewertung der Prüfungsleistung und die Bildung der Modulnote sind in § 10 der Prüfungsordnung geregelt.
Häufigkeit des Angebots	Das Modul wird mindestens einmal in jedem zweiten Studienjahr angeboten.
Arbeitsaufwand	Das Modul umfasst einen Gesamtarbeitsaufwand der Studenten von 120 AS.
Dauer des Moduls	Bei regulärem Studienverlauf erstreckt sich das Modul auf ein Semester.