

Vertiefungsmodul

Modulnummer	M10
Modulname	Kryptologie/Datensicherheit
Modulverantwortlich	Studiendekan der Fakultät für Mathematik
Inhalte und Qualifikationsziele	<p><u>Inhalte:</u></p> <ul style="list-style-type: none"> - 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 <p><u>Qualifikationsziele:</u> 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.</p>
Lehrformen	<p>Lehrformen des Moduls sind Vorlesung und Übung.</p> <ul style="list-style-type: none"> • V: Kryptologie/Datensicherheit (2 LVS) • Ü: Kryptologie/Datensicherheit (2 LVS)
Voraussetzungen für die Teilnahme	keine
Verwendbarkeit des Moduls	
Voraussetzungen für die Vergabe von Leistungspunkten	<p>Die Erfüllung der Zulassungsvoraussetzung für die Prüfungsleistung und die erfolgreiche Ablegung der Modulprüfung sind Voraussetzungen für die Vergabe von Leistungspunkten.</p> <p>Zulassungsvoraussetzung ist folgende Prüfungsvorleistung (mehrfach wiederholbar):</p> <ul style="list-style-type: none"> • Nachweis von 4 bis 14 Übungsaufgaben zu Kryptologie/Datensicherheit <p>Der Nachweis ist erbracht, wenn mindestens 40 % der geforderten Aufgaben richtig gelöst worden sind.</p>
Modulprüfung	<p>Die Modulprüfung besteht aus einer Prüfungsleistung:</p> <ul style="list-style-type: none"> • 90-minütige Klausur
Leistungspunkte und Noten	<p>In dem Modul werden 4 Leistungspunkte erworben.</p> <p>Die Bewertung der Prüfungsleistung und die Bildung der Modulnote sind in § 10 der Prüfungsordnung geregelt.</p>
Häufigkeit des Angebots	Das Modul wird mindestens einmal in jedem zweiten Studienjahr angeboten.
Arbeitsaufwand	Das Modul umfasst einen Gesamtarbeitsaufwand der Studierenden von 120 AS.
Dauer des Moduls	Bei regulärem Studienverlauf erstreckt sich das Modul auf ein Semester.