

Lehrende/r	Dr. Silke Hartlieb	Modulverantwortliche/r	Dr. Silke Hartlieb
	Dauer des Moduls ein Semester	ECTS 10	Workload 300 Stunden
			Häufigkeit in jedem Wintersemester
Lehrveranstaltung(en)	Mathematische Grundlagen der Kryptografie		
Detaillierter Zeitaufwand	Bearbeiten der Lektionen (7 mal 25 Stunden): 175 Stunden Einüben des Stoffes (z.B. durch Einsendeaufgaben): 75 Stunden Wiederholung und Prüfungsvorbereitung (u.a. Online-Tutorien): 50 Stunden		
Qualifikationsziele	Die Studierenden lernen klassische und aktuelle Verfahren der Kryptografie kennen und verstehen die mathematischen Hintergründe dieser Verfahren. Sie kennen die für den Bereich IT-Sicherheit wichtigsten Inhalte der Algebra und Elementaren Zahlentheorie und wissen, wie diese mathematischen Grundlagen in das Design von Kryptosystemen und in die Kryptoanalyse einfließen.		
Inhalte	<p>Die Kryptografie ist die Lehre von den Geheimschriften. Während diese bis vor wenigen Jahren eine Domäne des Militärs und der Diplomatie war, hält sie nun im Zuge der elektronischen Datenverarbeitung und Kommunikation mehr und mehr Einzug ins tägliche Leben. Neben der Aufgabe, Inhalte von Nachrichten vor der Nutzung von Unbefugten zu schützen, sind noch andere Aufgaben hinzugekommen, wie etwa sicherzustellen, dass eine Nachricht im Zuge der Übermittlung nicht geändert wurde, oder dass sie wirklich von dem angegebenen Absender stammt. In der Lehrveranstaltung werden zunächst klassische symmetrische Verfahren der Kryptografie vorgestellt. Im Zentrum stehen jedoch Public Key Verfahren, die hauptsächlich auf algebraischen und zahlentheoretischen Grundlagen basieren. Zu nennen sind elementare Gruppen- und Ringtheorie, Theorie endlicher Körper, Theorie ganzzahliger Gitter sowie modulare Arithmetik, Theorie elliptischer Kurven und Primzahltests. Diese Grundlagen werden bereitgestellt, und es wird gezeigt, wie sie in moderne Kryptosysteme einfließen und in der Kryptoanalyse eingesetzt werden.</p> <p>Die genauen Inhalte sind:</p> <ul style="list-style-type: none"> - Grundlagen der Algebra (Gruppen, Ringe, (endliche) Körper, elliptische Kurven) - Grundlagen der Elementaren Zahlentheorie - Asymmetrische Kryptosysteme (RSA-, Massey-Omura-, Diffie-Hellman-, ElGamal-, Kryptosystem, Kryptosysteme über elliptischen Kurven), - Primzahltests - Komplexität - Gitter (Basen, LLL-Algorithmus, Knapsack-Kryptosystem) 		
Inhaltliche Voraussetzung	Gute Kenntnisse des Moduls 61112 "Lineare Algebra" und des Moduls 61211 "Analysis". Die geforderten Voraussetzungen gehen über das hinaus, was in einem Studium der Informatik an Mathematikkenntnissen vermittelt wird.		
Lehr- und Betreuungsformen	Lehrveranstaltungsmaterial internetgestütztes Diskussionsforum Lehrvideos Einsendeaufgaben mit Korrektur und/oder Musterlösung Betreuung und Beratung durch Lehrende Zusatzmaterial Online-Tutorium		
Anmerkung	-		
Formale Voraussetzung	keine		
Vertiefungsrichtung	Angewandte Algebra und Diskrete Mathematik (AD)		

Verwendung des Moduls B.Sc. Mathematik
B.Sc. Mathematisch-technische Softwareentwicklung
M.Sc. Data Science
M.Sc. Informatik
M.Sc. Mathematik
M.Sc. Praktische Informatik

Prüfungsformen		Art der Prüfungsleistung	Voraussetzung
Prüfung		benotete mündliche Prüfung (ca. 25 Minuten)	keine
Stellenwert der Note	1/12		