Modulbezeichnung (Kürzel)	**Kryptologie** (KRYP)
Modulbezeichnung (eng.)	Cryptology
Semester (Häufigkeit)	WPM (jedes Sommersemester)
ECTS-Punkte (Dauer)	5 (1 Semester)
Art	Wahlpflichtmodul Zertifikat IT-Sicherheit
Studentische Arbeitsbelastung	60 h Kontaktzeit + 90 h Selbststudium
Voraussetzungen (laut BPO)	
Empf. Voraussetzungen	Java 1 oder C/C++
Verwendbarkeit	BI, BIPV
Prüfungsart und -dauer	Klausur 1,5 h oder oder mündliche Prüfung oder Kursarbeit
Lehr- und Lernmethoden	Vorlesung, Übung, Studentische Arbeit
Modulverantwortliche(r)	P. Felke

Qualifikationsziele
Die Studierenden kennen grundlegende Algorithmen für symmetrische und asymmetrische Verschlüsselung, sowie die wesentlichen Angriffsmethoden. Sie kennen Einsatzsszenarien von asymmetrischer, symmetrischer Kryptographie sowie Hashfunktionen und sind dadurch in der Lage, praktische Verfahren zu bewerten bzw. geeignete Verfahren für bestimmte Anwendungszwecke auszuwählen. Sie kennen typische Algorithmen zur Implementation von Kryptosystemen und Fallstricke bei der Umsetzung.

Lehrinhalte
Symmetrische und asymmetrische Kryptographie sowie Hashfunktionen werden vorgestellt. Die mathematischen, algorithmischen und kryptoanalytischen Aspekte werden diskutiert.

Literatur
Paar, C., Pelzl, J.: Kryptografie verständlich, Springer 2016
Buchmann, J.: Einführung in die Kryptographie, Springer 2010
Stinson, D.: Cryptography, Theory and Practice, fourth Edition, CRC Press 2019

Lehrveranstaltungen

Dozenten/-innen	**Titel der Lehrveranstaltung**	**SWS**
P. Felke	Kryptologie	2
P. Felke	Übung Kryptologie	2