Modulbezeichnung	**Kryptologie**
Semester	WPF
Dauer	1 Semester
Art	Wahlpflichtmodul Zertifikat IT-Sicherheit
ECTS-Punkte	5
Studentische Arbeitsbelastung	60 h Kontaktzeit + 90 h Selbststudium
Voraussetzungen (laut BPO)	Mathematik 1
Empf. Voraussetzungen	
Verwendbarkeit	BI
Prüfungsform und -dauer	Klausur 1,5 h oder mündliche Prüfung oder Kursarbeit
Lehr- und Lernmethoden	Vorlesung, Übung, Studentische Arbeit
Modulverantwortlicher	P. Felke
Qualifikationsziele	Die Studierenden kennen grundlegende Algorithmen für symmetrische und asymmetrische Verschlüsselung sowie die wesentlichen Angriffsmethoden. Sie kennen Einsatzszenarien von asymmetrischer, symmetrischer Kryptographie sowie Hashfunktionen und sind dadurch in der Lage praktische Verfahren zu bewerten bzw. geeignete Verfahren für bestimmte Anwendungszwecke auswählen. 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

Dozent	**Titel der Lehrveranstaltung**	**SWS**
P. Felke	Kryptologie	4