Modulbezeichnung	**Kryptologie**
Semester	WPF
ECTS-Punkte (Dauer)	5 (1 Semester)
Art	Wahlpflichtfach Zertifikat IT-Sicherheit
Studentische Arbeitsbelastung	60 h Kontaktzeit + 90 h Selbststudium
Voraussetzungen (laut BPO)	
Empf. Voraussetzungen	Mathematik 1, Mathematik 2, Mathematik 3, C/C++
Verwendbarkeit	BaI
Prüfungsform und -dauer	Klausur 1,5 h oder mündliche Prüfung
Lehr- und Lernmethoden	Vorlesung, Studentische Arbeit
Modulverantwortlicher	G. Brands

Qualifikationsziele
Die Studenten kennen den Aufbau der wesentlichen Basisalgorithmen für Einweg-, symmetrische und asymmetrische Verschlüsselung sowie die wesentlichen bekannten Angriffsmethoden. Sie können anwendungsbedingt Hybridverfahren bewerten bzw. geeignete Hybridverfahren für bestimmte Anwendungszwecke auswählen. Sie kennen geeignete Algorithmen zur Implementation von Verfahren auf Rechnern. Sie kennen unterschiedliche Authentifizierungsmethoden und haben wesentliche in der Praxis eingesetzte Mechanismen experimentell erprobt.

Lehrinhalte
Hashalgorithmen der aktuellen und der zukünftigen Generation, ihre Einsatzbereiche und Gefährdungen werden vorgestellt, desgleichen symmetrische Verschlüsselungsverfahren. Die mathematischen Grundlagen und ihre Übersetzung in Computeralgorithmen für symmetrische Verfahren werden ausführlich bis hin zu komplexeren Authentifizierungen diskutiert.

Literatur
Brands, G.: Verschlüsselungsalgorithmen, Vieweg 2001
Brands, G.: Verschlüsselung, Signaturen, Angriffsmethoden, Books on Demand, 2. Auflage 2014

Lehrveranstaltungen

Dozent	**Titel der Lehrveranstaltung**	**SWS**
G. Brands	Kryptologie	4