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	Programmieren 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 und sind dadurch in der Lage geeignete Verfahren für bestimmte Anwendungszwecke auszuwählen. Die Studierenden können moderne Kryptosysteme mit den gelernten Angriffstechniken kryptoanalysieren und entsprechende Hilfsprogramme erstellen. Sie sind dadurch in der Lage die Güte von Verfahren hinsichtlich dieser Angriffe zu bewerten. Sie kennen typische, effiziente Algorithmen zur Implementation von Kryptosystemen und Fallstricke bei der Umsetzung bzw. beim Einsatz in Übertragungsprotokollen. Die Studierenden sind dadurch auch in der Lage, die eingesetzen kryptographischen Verfahren in typischen Übertragungsprokollen, wie z.B. TLS, sicherheitlich zu bewerten.

Lehrinhalte
Symmetrische und asymmetrische Kryptographie, wie z.B. AES, RSA und die Familie der SHA-Hashfunktionen, werden vorgestellt. Die mathematischen, algorithmischen und kryptoanalytischen Aspekte werden erläutert. Es werden die Einsatzzwecke, z.B. in Übertragungsprotokollen, erklärt und diskutiert. Die Angriffe bzw. kryptoanalytischen Ansätze, so wie die Verfahren selbst werden im Praktikum vertieft, bewertet und implementiert.

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