MK105 - Advanced Cryptography

MK105 - Advanced Cryptography

Allgemeine Informationen	
Modulkürzel oder Nummer	MK105
Eindeutige Bezeichnung	
Modulverantwortlich(e)	Prof. Dr. Jetzek, Ulrich (ulrich.jetzek@haw-kiel.de)
Lehrperson(en)	Prof. Dr. Jetzek, Ulrich (ulrich.jetzek@haw-kiel.de)
Wird angeboten zum	Sommersemester 2022
Moduldauer	1 Fachsemester
Angebotsfrequenz	Regelmäßig
Angebotsturnus	In der Regel im Sommersemester
Lehrsprache	Englisch
Empfohlen für internationale Studierende	Ja
Ist als Wahlmodul auch für andere Studiengänge freigegeben (ggf. Interdisziplinäres Modulangebot - IDL)	Nein

Studiengänge und Art des Moduls (gemäß Prüfungsordnung)
Studiengang: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Vertiefungsrichtung: Kommunikationstechnik und Embedded Systems Modulart: Wahlmodul Fachsemester: 1, 2
Studiengang: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Vertiefungsrichtung: Mechatronik Modulart: Wahlmodul Fachsemester: 1, 2
Studiengang: M.Sc. - MIE - Information Engineering (PO 2022, V3) Vertiefungsrichtung: IT Security Modulart: Wahlmodul Fachsemester: 1, 2, 3
Studiengang: M.Sc. - MIE - Information Engineering (PO 2022, V3) Vertiefungsrichtung: Intelligent Systems Modulart: Wahlmodul Fachsemester: 1, 2, 3
Studiengang: M.Sc. - MIE - Information Engineering (PO 2022, V3) Vertiefungsrichtung: Information Technology and Systems Modulart: Wahlmodul Fachsemester: 1, 2, 3

Kompetenzen / Lernergebnisse
Kompetenzbereiche: Wissen und Verstehen; Einsatz, Anwendung und Erzeugung von Wissen; Kommunikation und Kooperation; Wissenschaftliches Selbstverständnis/Professionalität.

Students have understood the basic concepts of modern symmetric cryptosystems, i.e. they have understood the principle of confusion and diffusion elements in symmetric cryptosystems. The students have understood the basic concept of asymmetric cryptosystems, i.e. they know what a one-way- or trapdoor-function is and how it is applied in asymmetric cryptosystems. In particular the students know what the integer factorization problem is. In addition they know how encryption based on the Discrete Logarithm Problem (DLP) and how encryption based on Elliptic Curve Cryptography (ECC) works. Furthermore they know the basic concepts of hash functions and digital signatures.
In particular the students have good insight into the Data Encryption Standard (DES) as well as into the Advanced Encryption Standard (AES). Furthermore the students know the principle of and requirements for stream ciphers, in particular of the A5/1-stream cipher. The students know how encryption and decryption in the RSA system work. Furthermorre the students have understood the Diffie-Hellman-Key-Exchange. Based on the above knowledge students will be able to perform implementation tasks within the field of modern cryptography.
Students shall communicate and discuss the above mentioned topics in order to share their knowledge with others and to gain a deeper understanding of cryptography.

Angaben zum Inhalt

Lehrinhalte	- introduction, historic ciphers, general principles of modern symmetric crypto systems - number theory, Galois fields, extension fields - encryption and decryption methods of symmetric and asymmetric cryptography, as e.g. - DES (Data Encryption Standard) - AES (Advanced Encryption Standard) - Public key methods (RSA) - Digital signatures and hash functions. - ECC (elliptic curve cryptography)
Literatur	- Jan Pelzl, Christof Paar: „Understanding Cryptography“, Springer-Verlag, 2010 - Johannes Buchmann: „Einführung in der Kryptographie“, Springer-Verlag 2008, 4. Auflage - Klaus Schmeh: „Kryptografie – Verfahren, Protokolle, Infrastrukturen“, dpunkt Verlag 2009, 4. Auflage - CryptToolSkript, Mathematik und Kryptographie, http://www.cryptool.de/

Lehrformen der Lehrveranstaltungen

Lehrform	SWS
Übung	2
Lehrvortrag	2

Arbeitsaufwand

Anzahl der SWS	4 SWS
Leistungspunkte	5,00 Leistungspunkte
Präsenzzeit	48 Stunden
Selbststudium	102 Stunden

Modulprüfungsleistung

Voraussetzung für die Teilnahme an der Prüfung gemäß PO	Keine

MK105 - Übung	Prüfungsform: Übung Gewichtung: 30% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Ja
MK105 - Klausur	Prüfungsform: Klausur Dauer: 90 Minuten Gewichtung: 70% wird angerechnet gem. § 11 Absatz 2 PVO: Ja Benotet: Ja