HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

MK105 - Advanced Cryptography

MK105 - Advanced Cryptography

General information	
Module Code	MK105
Unique Identifier	
Module Leader(s)	Prof. Dr. Jetzek, Ulrich (ulrich.jetzek@haw-kiel.de)
Lecturer(s)	Prof. Dr. Jetzek, Ulrich (ulrich.jetzek@haw-kiel.de)
Offered in Semester	Sommersemester 2022
Module duration	1 Semester
Occurrence frequency	Regular
Module occurrence	In der Regel im Sommersemester
Language	Englisch
Recommended for international students	Yes
Can be attended with different study programme	No

Curricular relevance (according to examination regulations)
Study Subject: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Study Specialization: Kommunikationstechnik und Embedded Systems Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Eng. - MET - Elektrische Technologien (PO 2017, V3) Study Specialization: Mechatronik Module type: Wahlmodul Semester: 1, 2
Study Subject: M.Sc. - MIE - Information Engineering (PO 2022, V3) Study Specialization: IT Security Module type: Wahlmodul Semester: 1, 2, 3
Study Subject: M.Sc. - MIE - Information Engineering (PO 2022, V3) Study Specialization: Intelligent Systems Module type: Wahlmodul Semester: 1, 2, 3
Study Subject: M.Sc. - MIE - Information Engineering (PO 2022, V3) Study Specialization: Information Technology and Systems Module type: Wahlmodul Semester: 1, 2, 3

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
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.

Content information	
Content	- 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)
Literature	- 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/

Teaching formats of the courses	
Teaching format	**SWS**
Übung	2
Lehrvortrag	2

Workload	
Number of SWS	4 SWS
Credits	5,00 Credits
Contact hours	48 Hours
Self study	102 Hours

Module Examination	
Examination prerequisites according to exam regulations	None
MK105 - Übung	Method of Examination: Übung Weighting: 30% wird angerechnet gem. § 11 Absatz 2 PVO: Yes Graded: Yes
MK105 - Klausur	Method of Examination: Klausur Duration: 90 Minutes Weighting: 70% wird angerechnet gem. § 11 Absatz 2 PVO: Yes Graded: Yes