Module title			Abbreviation
Cryptography and Data Security			10-GE-KD-162-m01
Module coordinator		**Module offered by**	
Dean of Studies Informatik (Computer Science)		Institute of Computer Science	
ECTS	**Method of grading**	**Only after succ. compl. of module(s)**	
5	numerical grade	--	
Duration	**Module level**	**Other prerequisites**	
1 semester	undergraduate	--	

Contents

Private key cryptography systems, Vernam one-time pad, AES, perfect security, public key cryptography systems, RSA, Diffie-Hellman, Elgamal, Goldwasser-Micali, digital signature, challenge-response methods, secret sharing, millionaire problem, secure circuit evaluation, homomorphous encryption.

Intended learning outcomes

The students possess a fundamental and applicable knowledge in the areas of private key cryptography systems, Vernam one-time pad, AES, perfect security, public key cryptography, RSA, Diffie-Hellman, Elgamal, Goldwasser-Micali, digital signature, challenge-response method, secret sharing, millionaire problem, secure circuit evaluation, homomorphous encryption

Courses (type, number of weekly contact hours, language — if other than German)

V (2) + Ü (2)

Method of assessment (type, scope, language — if other than German, examination offered — if not every semester, information on whether module is creditable for bonus)

written examination (approx. 60 to 120 minutes).
If announced by the lecturer at the beginning of the course, the written examination may be replaced by an oral examination of one candidate each (approx. 20 minutes) or an oral examination in groups of 2 candidates (approx. 15 minutes per candidate).
Language of assessment: German and/or English
creditable for bonus

Allocation of places

--

Additional information

--

Workload

150 h

Teaching cycle

--

Referred to in LPO I (examination regulations for teaching-degree programmes)

--

Module appears in

Bachelor' degree (1 major) Games Engineering (2016)
Bachelor' degree (1 major) Games Engineering (2017)