Module title: Cryptography and Data Security
Abbreviation: 10-I=KD-161-m01

Module coordinator: Dean of Studies Informatik (Computer Science)
Module offered by: Institute of Computer Science

ECTS: 5
Method of grading: numerical grade
Duration: 1 semester
Module level: graduate
Other prerequisites: --

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, homomorphic 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, homomorphic encryption.

Courses:
(V) (2) + Ü (2)

Method of assessment:
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).
Separate written examination for Master’s students.
Language of assessment: German and/or English creditable for bonus

Allocation of places:
--

Additional information:
Focuses available for students of the Master’s programme Informatik (Computer Science, 120 ECTS credits): AL, SE, IT, IS.

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

Module appears in:
Master’s degree (1 major) Computer Science (2016)
Master’s degree (1 major) Computer Science (2017)
Master’s degree (1 major) Computer Science (2018)