Module title			Abbreviation
Cryptography and Data Security			10-I=KD-102-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	graduate	Where applicable, prerequisites as specified by the lecturer at the beginning of the course (e. g. completion of exercises).

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 + Ü (no information on SWS (weekly contact hours) and course language available)

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. 50 to 60 minutes); if announced by the lecturer by four weeks prior to the examination date, the written examination can be replaced by an oral examination of one candidate each or an oral examination in groups (one candidate each: 15 minutes, groups of 2: 20 minutes, groups of 3: 25 minutes)
Language of assessment: German, English if agreed upon with the examiner

Allocation of places

--

Additional information

--

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

--

Module appears in

Master's degree (1 major) Computer Science (2010)
Master's degree (1 major) Mathematics (2012)
Master's degree (1 major) Mathematics (2010)
Master's degree (1 major) Computational Mathematics (2012)
First state examination for the teaching degree Gymnasium Computer Science (2009)