

<b>Module title</b>		<b>Abbreviation</b>
Cryptography and Data Security		10-I-KD-141-m01
<b>Module coordinator</b>		<b>Module offered by</b>
Dean of Studies Informatik (Computer Science)		Institute of Computer Science
<b>ECTS</b>	<b>Method of grading</b>	<b>Only after succ. compl. of module(s)</b>
5	numerical grade	--
<b>Duration</b>	<b>Module level</b>	<b>Other prerequisites</b>
1 semester	undergraduate	--
<b>Contents</b>		
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.		
<b>Intended learning outcomes</b>		
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		
<b>Courses</b> (type, number of weekly contact hours, language – if other than German)		
V + Ü (no information on SWS (weekly contact hours) and course language available)		
<b>Method of assessment</b> (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 can be replaced by an oral examination of one candidate each (approx. 20 minutes) or an oral examination in groups (groups of 2, approx. 30 minutes) Language of assessment: German, English		
<b>Allocation of places</b>		
--		
<b>Additional information</b>		
--		
<b>Referred to in LPO I</b> (examination regulations for teaching-degree programmes)		
--		
<b>Module appears in</b>		
Bachelor' degree (1 major) Computer Science (2014)		