Modulbezeichnung:	Cryptography
Studiensemester:	1st
Modulverantwortlicher:	Professor Dr. Joachim von zur Gathen
Dozent(in):	Professor Dr. Joachim von zur Gathen, Dr. Michael Nüsken
Sprache:	English
Zuordnung zum Curriculum:	Media Informatics
Lehrform/SWS: *(und Gruppengrößen)*	V4 Ü2 or V3 Ü2
Arbeitsaufwand:	240h or 180h
Kreditpunkte:	8 or 6
Voraussetzungen nach Prüfungsordnung:	None.
Empfohlene Voraussetzungen:	None.
Angestrebte Lernergebnisse:	Knowledge: On successful completion of this module, students should be able to – recall basic symmetric and asymmetric cryptosystems – describe the interplay between computing power and security requirements – state security goals and adverserial powers Skills: They should be able to – implement and use cryptographic primitives – use results from mathematics – present solutions orally (in tutorial groups) and in written form (homework assignments) Competences: Based on the knowledge and skills acquired they should be able to – discuss modern cryptosystems – identify problems in cryptographic protocols and implementations
Inhalt:	Basic private-key and public-key cryptosystems: AES, RSA, group-based. Security reductions. Key exchange, cryptographic hash functions, signatures, identification; Factoring integers and discrete logging; Lower bounds in structured models.
Studien-/Prüfungsleistungen:	Written exam (oral exam in exceptional cases)
Medienformen:	none
Literatur:	Stinson, Cryptography: Theory and Practice, 2nd edition