Modulbezeichnung:	The Art of Cryptography
Studiensemester:	2nd
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)*	V4Ü2 or V3Ü2
Arbeitsaufwand:	240h or 180h
Kreditpunkte:	8 or 6
Voraussetzungen nach Prüfungsordnung:	
Empfohlene Voraussetzungen:	Cryptography
Angestrebte Lernergebnisse:	Knowledge: On successful completion of this module, students should be able to – define terms for the theoretical foundations behind modern cryptography – recall proofs for security reductions – describe techniques of advanced cryptanalysis Skills: They should be able to – implement and use cryptographic primitives – use results from advanced mathematics and complexity theory – 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 theoretical foundations of cryptography – critically assess current research
Inhalt:	Possible topics are - pseudorandomness and zero-knowledge, - security reductions, - lattices.
Studien-/Prüfungsleistungen:	Written exam (oral exam in exceptional cases)
Medienformen:	none
Literatur:	Varying