Module MA-INF 1312	**The Art of Cryptography**				
Workload 270 h	**Credit points** 9 CP	**Duration** 1 semester	**Frequency** every year		
Module coordinator	Prof. Dr. Joachim von zur Gathen				
Lecturer(s)	Prof. Dr. Joachim von zur Gathen, Dr. Michael Nüsken				
Classification	**Programme** M. Sc. Computer Science	**Mode** Optional	**Semester** 2.		
Technical skills	Insights into the theoretical foundations behind security concerns and measures, and of the interplay between computing power, and security requirements. Mastery of advanced techniques for cryptosystems and cryptanalysis.				
Soft skills	Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment				
Contents	Possible topics are • pseudorandomness and zero-knowledge, • security reductions, • lattices.				
Prerequisites	**Recommended:** MA-INF 1103 – Cryptography				
Format	**Teaching format**	**Group size**	**h/week**	**Workload[h]**	**CP**
	Lecture	60	4	60 T / 105 S	5.5
	Exercises	30	2	30 T / 75 S	3.5
	T = face-to-face teaching; S = independent study				
Exam achievements	Written exam (graded)				
Study achievements	Successful exercise participation (not graded)				
Forms of media					
Literature	Varying				