Module title			Abbreviation
Mathematical Aspects of Modern Cryptography			10-M-KRY-232-m01
Module coordinator		**Module offered by**	
Dean of Studies Mathematik (Mathematics)		Institute of Mathematics	
ECTS	**Method of grading**	**Only after succ. compl. of module(s)**	
5	(not) successfully completed	--	
Duration	**Module level**	**Other prerequisites**	
1 semester	undergraduate	--	

Contents

Fundamentals of elementary number theory, public key cryptography, the mathematics of quantum computers, Shor's factorization algorithm, post-quantum cryptography.

Intended learning outcomes

The student knows the essential methods and basic concepts of elementary number theory, their application in public-key cryptosystems, and computational methods and algorithms for quantum computers.

Courses (type, number of weekly contact hours, language — if other than German)

V (3) + Ü (1)

Method of assessment (type, scope, language — if other than German, examination offered — if not every semester, information on whether module is creditable for bonus)

a) written examination (approx. 60 to 120 minutes, usually chosen) or
b) oral examination of one candidate each (15 to 30 minutes) or
c) oral examination in groups (groups of 2, 10 to 15 minutes per candidate)
Language of assessment: German and/or English
Assessment offered: Only when announced in the semester in which the courses are offered and in the subsequent semester
creditable for bonus

Allocation of places

--

Additional information

--

Workload

150 h

Teaching cycle

--

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

--

Module appears in

exchange program Mathematics (2023)
First state examination for the teaching degree Gymnasium Mathematics (2023)
Bachelor' degree (1 major) Mathematics (2023)
Bachelor' degree (1 major) Mathematical Physics (2024)