UNIVERSITÄT
BIELEFELD

Module Guide
24-M-ND-STCR Selected Topics of Cryptography

Fakultät für Mathematik

Version dated Dec 14, 2025

This module guide reflects the current state and is subject to change. Up-to-date information and the latest version of this document can be found online via the page

https://ekvv.uni-bielefeld.de/sinfo/publ/modul/533561038

The current and valid provisions in the module guide are binding and further specify the subject-related regulations (German "FsB") published in the Official Announcements of Bielefeld University.

24-M-ND-STCR Selected Topics of Cryptography

Faculty

Fakultät für Mathematik

Person responsible for module

Frau PD Dr. Barbara Baumeister

Regular cycle (beginning)

This module is part of a long-term overall curriculum plan for the Master's programme, which ensures that modules with an amount of at least 20 CP are offered in all five fields each year. The module is offered at irregular intervals as part of this overall curriculum planning.

Credit points

10 Credit points

Competencies

Non-official translation of the module descriptions. Only the German version is legally binding.

Students master advanced content and methods of Cryptography, in particular they can independently carry out very complex proofs with reference to current research questions
in this area, requiring a high level of mathematical expertise. Students are able to describe central concepts and methods of combinatorial group theory, non-commutative cryptography, the theory of platform groups and post-quantum cryptography and apply them in different contexts.

Students will be introduced to current research questions in the area of Cryptography. They are able to recognise and assess further development opportunities and research goals.
Furthermore, students recognise further-reaching connections to mathematical issues that have already been worked out. They can transfer and apply the knowledge and methods they have learnt so far to deeper mathematical problem areas. Students also expand their mathematical intuition as a result of more intensive study.
In combination with other in-depth modules, they will be able to write their own research papers, e.g. a master's thesis in the field of Cryptography.
In the tutorials, students develop their ability to discuss mathematical topics and thus further prepare themselves for the requirements of the Master's module, in particular for the scientific discussion within the Master's seminar presentation and the defence of their Master's thesis.

Content of teaching

The following advanced content of teaching in the field of cryptography is covered:

- Combinatorial group theory (representations of groups by generators and relations, algorithmic group-theoretic problems, Nielsen algorithm, Reidemeister-Schreier algorithm, the isomorphism problem and Tietze's solution).

- Non-commutative cryptography

- Platform groups (theory of Zopf groups with normal form, conjugacy problem, Garside groups)
- Post-quantum-cryptography

This module prepares the content of a master's thesis.

Recommended previous knowledge

Knowledge of coding theory (24-M-ND-CTH) and cryptography (24-M-ND-CRY)

Necessary requirements

–

Explanation regarding the elements of the module

Module structure: 1 SL, 1 bPr [1]

Courses

Title	Type	Regular cycle	Workload [5]	LP[2]
Lecture Selected Topics of Cryptography	lecture	This module is part of a long-term overall curriculum plan for the Master's programme, which ensures that modules with an amount of at least 20 CP are offered in all five fields each year. The module is offered at irregular intervals as part of this overall curriculum planning.	60 h (60 + 0)	2 [Pr]

Tutorials Selected Topics of Cryptography	exercise	This module is part of a long-term overall curriculum plan for the Master's programme, which ensures that modules with an amount of at least 20 CP are offered in all five fields each year. The module is offered at irregular intervals as part of this overall curriculum planning.	90 h (30 + 60)	3 [SL]

Study requirements

Allocated examiner	Workload	LP[2]
Teaching staff of the course **Tutorials Selected Topics of Cryptography (exercise)** *Regular completion of the exercises, each with a recognisable solution approach, as well as participation in the exercise groups for the module's lecture. As a rule, participation in the exercise group includes presenting solutions to exercises twice after being asked to do so as well as regular contributions to the scientific discussion in the exercise group, for example in the form of comments and questions on the proposed solutions presented. The organiser may replace some of the exercises with face-to-face exercises.*	see above	see above

Examinations

Allocated examiner	Type	Weighting	Workload	LP[2]
Teaching staff of the course **Lecture Selected Topics of Cryptography (lecture)** *(electronic) written examination in presence of usually 120 minutes, oral examination in presence or remote of usually 40 minutes, A remote electronic written examination is not permitted.*	e-Klausur o. Klausur o. mündliche e-Prüfung o. mündliche Prüfung	1	150h	5

Legend

1 The module structure displays the required number of study requirements and examinations.

2 LP is the short form for credit points.

3 The figures in this column are the specialist semesters in which it is recommended to start the module. Depending on the individual study schedule, entirely different courses of study are possible and advisable.

4 Explanations on mandatory option: "Obligation" means: This module is mandatory for the course of the studies; "Optional obligation" means: This module belongs to a number of modules available for selection under certain circumstances. This is more precisely regulated by the "Subject-related regulations" (see navigation).

5 Workload (contact time + self-study)

SoSe Summer semester

WiSe Winter semester

SL study requirement

Pr Examination

bPr Number of examinations with grades

uPr Number of examinations without grades