Dr: 2022/2503-3.1.2.2

Course syllabus

Faculty of Technology

Department of Mathematics

4MA423 Matematisk kryptering, 7.5 credits
Mathematical cryptography

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
Second Level

Progression
A1F

Date of Ratification
Approved 2015-05-22
Revised 2022-06-13 by Faculty of Technology. Examination (assessment methods) are revised.
The course syllabus is valid from spring semester 2023

Prerequisites
4MA421 Algebraic structures II, 7.5 credits or equivalent.

Objectives

The student should be able to:

- describe the encryption and decryption process of some modern cryptosystems
- describe some mathematical results which are of importance when it comes to cryptological applications
- solve problems and perform calculations within cryptology, and implement cryptological algorithms using mathematical software
- analyze and discuss ethical implications of cryptology, and the role played by cryptology within the society
- show deeper knowledge for some area within cryptology.

Content

Some historical ciphers. Discrete logarithms; ElGamal's cryptosystem, Diffie-Hellman's protocol. The RSA cryptosystem; primality testing methods, factorization methods. Information theory. Elliptic curve cryptography. Lattice-based cryptography. Pseudo-random number generators. The role of cryptology within the society.

Type of Instruction

Lectures and seminars.

Examination

The course is assessed with the grades A, B, C, D, E, Fx or F.

The grade A constitutes the highest grade on the scale and the remaining grades follow in descending order where the grade E is the lowest grade on the scale that will result in a pass. The grade F means that the student’s performance is assessed as fail (i.e. received the grade F).

The student's knowledge is assessed in the form of

- written assignments, of which some are laboratory; 3 credits (grading scale U/G)
- written project report that also is to be presented orally at a seminar; 2.5 credits (grading scale A-F)
- oral exam; 2 credits (grading scale A-F)

The final grade of the course is a weighted average of the grades on the written report and the oral exam.

Repeat examination is offered in accordance with Local regulations for courses and examination at the first and second-cycle level at Linnaeus University.If the university has decided that a student is entitled to special pedagogical support due to a disability, the examiner has the right to give a customised exam or to have the student conduct the exam in an alternative way.

Course Evaluation

During the implementation of the course or in close conjunction with the course, a course evaluation is to be carried out. Results and analysis of the course evaluation are to be promptly presented as feedback to the students who have completed the course. Students who participate during the next course instance receive feedback at the start of the course. The course evaluation is to be carried out anonymously.

Credit Overlap

The course cannot be included in a degree along with the following course/courses of which the content fully, or partly, corresponds to the content of this course: 4MA123 Mathematical cryptography, 7.5 credits

Other

Grade criteria for the A–F scale are communicated to the student through a special document. The student is to be informed about the grade criteria for the course by the start of the course at the latest.

Required Reading and Additional Study Material

Required reading

Hoffstein, Pipher & Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008 or later. 350 (523) pages.