Jnr: 2015/2072-3.1.2

Course syllabus

Faculty of Technology
Department of Mathematics

4MA423 Matematisk kryptering, 7,5 högskolepoäng
Mathematical cryptography, 7.5 credits

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
Second Level

Progression
A1F

Date of Ratification
Approved by Faculty of Technology 2015-05-22
The course syllabus is valid from spring semester 2016

Prerequisites
4MA121 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 (4.5 credits), of which some are laboratory (computer programming), and a written project (3 credits) that also is to be presented orally at a seminar.

To pass the course, the student must fulfill the objectives of the course.

Course Evaluation

During the course or in close connection to the course, a course evaluation is to be carried out. The result and analysis of the course evaluation are to be communicated to the students who have taken the course and to the students who are to participate in the course the next time it is offered. The course evaluation is carried out anonymously. The compiled report will be filed at the Faculty.

Credit Overlap

This course cannot be part of a degree in combination with another course in which the content fully or partly correspond 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.