Linnæus University

Dnr: 2014/2411 -3.1.2

Course syllabus

Faculty of Technology

Department of Mathematics

4MA123 Matematisk kryptering, 7,5 högskolepoäng
4MA123 Mathematical cryptography, 7.5 credits

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
Second Level

Progression
A1F

Date of Ratification
Approved 2010-12-10
Revised 2014-09-03 by Faculty of Technology. Prerequisites, objectives, content, examination and type of instructions are revised.
The course syllabus is valid from autumn semester 2015

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 Fail (U), Pass (G) or Pass with Distinction (VG).

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.

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

On request, students may have their credits translated to ECTS-marks. Such a request must be sent to the examiner before the grading process starts.

Course Evaluation
A course evaluation will be carried out at the end of the course in accordance with the guidelines of the University. The result of the course evaluation will be filed at the department.

Required Reading and Additional Study Material
Required reading
Hoffstein, Pipher & Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008 or later. 350 (523) pages.