Linnæus University

Course syllabus

Faculty Board of Science and Engineering
School of Computer Science, Physics and Mathematics

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

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
Second Level

Progression
A1N

Date of Ratification
Approved by the Board of the School of Computer Science, Physics and Mathematics 2010-12-10

The course syllabus is valid from spring semester 2011

Prerequisites
120 credits in mathematics, including courses in Algebraic Structures I 7.5 credit (2MA105) and Elementary Number Theory 7.5 creidts (2MA106), or equivalent.

Expected learning outcomes
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.

Content
Some Historical Ciphers. Discrete Logarithms; ElGamal's Cryptosystem, Diffie-Hellman's protocol. The RSA cryptosystem; Factorization Methods. Information Theory. Elliptic Curve Cryptography. Lattice-based Cryptography. Pseudo-random Number Generators.

Type of Instruction
Lectures and seminars. Compulsory assignments may be given during the course.

Examination
The course is assessed with the grades Fail (U), Pass (G) or Pass with Distinction (VG).
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.

The student's knowledge is assessed in the form of oral and/or written examinations. Furthermore, continuos assessment by written and/or oral representation can be used during the course. The principal assessment method for the course is determined at the beginning of the course.

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.