Linnæus University

Dnr: 2014/2430 -3.1.2

Course syllabus

Faculty of Technology

Department of Mathematics

1MA164 Kryptering och kodningsteori, 7,5 högskolepoäng
1MA164 Cryptography and Coding Theory, 7.5 credits

Main field of study
Mathematics

Subject Group
Mathematics

Level of classification
First Level

Progression
G1F

Date of Ratification
Approved 2009-08-11
Revised 2014-09-03 by Faculty of Technology. Objectives, content, examination and type of instructions are revised.
The course syllabus is valid from spring semester 2015

Prerequisites
Basic Mathematics (1MA101), 7.5 credits and Vector Geometry (1MA103), 7,5 hp or Basic Mathematics for Computer Scientists (1MA141), 7.5 credits or equivalent.

Objectives

The student should be able to:

- describe some common algorithms for ciphers and codes
- describe the strengths and weaknesses of different ciphers
- use cryptanalysis to break classical ciphers
- understand the principles for coding and decoding of error correcting codes.

Content

Cryptorgaphy:

Some classical cryptosystems, e.g. affine ciphers, substitution ciphers, the Vigenère cipher, and the Hill cipher.

Data Encryp-tion Standard (DES). Advanced Encryption Standard (AES). Public Key

Cryptosystems, especially the RSA algorithm and the ElGamal Cryptosystem. Digital Signatures. Diffie-Hellman's protocol.

Orientation on current research issues

Coding theory:

Error correcting codes. Linear codes. Hamming codes. Cyclic codes. The CRC algorithm.

Type of Instruction

Lectures and exercise and laboratory sessions.

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 a written exam and a written presentation of a computer assignment.

Course Evaluation

A written 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

Trappe, W & Washington, L C. *Introduction to Cryptography with Coding Theory*, 2nd Ed., Pearson Education, 2006 or later. 250 (577) pages.

DFM: Distributed material, Linnæus University, current year. 30 pages.