



Course syllabus

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

1MA164 Kryptering och kodningsteori, 7,5 högskolepoäng
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 by the Board of the School of Computer Science, Physics and Mathematics
2009-08-11

Revised 2010-04-23

The course syllabus is valid from spring semester 2011

Prerequisites

60 credits in Mathematics, including courses in basic mathematics (1MA101), 7.5 credits and Vector Geometry (1MA103), 7.5 credits or equivalent.

Expected learning outcomes

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

Cryptography:

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

Data Encryption Standard (DES). Advanced Encryption Standard (AES). Public Key Cryptosystems, especially the RSA algorithm and the ElGamal Cryptosystem. Digital Signatures. Diffie-Hellman's protocol.

Coding theory:

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

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. There could also be a continuous examination in the form of oral and/or written reports throughout the course. The principal assessment method for the course is determined at the beginning of the course.

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.