Linnæus University

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 Organisational Committee 2009-08-11

The course syllabus is valid from spring semester 2010

Prerequisites
One year of full-time study in Mathematics (equivalent to 60 higher education credits), including courses in basic mathematics (1MA101) and Vector Geometry (1MA103), 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

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.

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.

Assessment methods The student's knowledge is assessed in the form of oral and/or written examinations. The principal assessment method for the course is determined at the beginning of the course.

Course Evaluation

After the course a written evaluation of the course will take place according to the University guidelines.

Required Reading and Additional Study Material

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

MSI:Separate handouts. 30