Linnæus University

Jnr: 2022/200-3.1.2.2

Course syllabus

Faculty of Technology
Department of Mathematics

1MA464 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 2015-05-22
Revised 2022-01-24 by Faculty of Technology. Literature list is revised.
The course syllabus is valid from spring semester 2022

Prerequisites
1MA462 Discrete Mathematics, or equivalent.

Objectives

After completing the course, the student should be able to

- solve problems, perform calculations, and conduct lines of reasoning within the part of mathematics that is covered by the course, and to communicate those solutions, calculations, and reasonings in writing
- identify and formulate problems within the field of the course and carry out exercises within given time limits.

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 seminars.

Examination

The course is assessed with the grades A, B, C, D, E, Fx or F.
The grade A constitutes the highest grade on the scale and the remaining grades follow in descending order where the grade E is the lowest grade on the scale that will result in a pass. The grade F means that the student's performance is assessed as fail (i.e. received the grade F).

The student's knowledge is assessed in form of a written exam, along with a computer project.

Course Evaluation

During the course or in close connection to the course, a course evaluation is to be carried out. The result and analysis of the course evaluation are to be communicated to the students who have taken the course and to the students who are to participate in the course the next time it is offered. The course evaluation is carried out anonymously. The compiled report will be filed at the Faculty.

Credit Overlap

The course cannot be included in a degree along with the following courses of which the content fully, or partly, corresponds to the content of this course: 1MA164 Cryptography and Coding Theory, 7.5 credits

Other

Grade criteria for the A–F scale are communicated to the student through a special document. The student is to be informed about the grade criteria for the course by the start of the course at the latest.

Required Reading and Additional Study Material

Required Reading

Christof Paar & Jan Pelzl. *Understanding Cryptography*, Springer, latest edition. 140 (350) pages.

Simon Rubinstein-Salzedo: *Cryptography*, Springer, latest edition. 65 (250) pages

FTK: Distributed material, Linnæus University, current year. 58 pages.