DD2448 Foundations of Cryptography 7.5 credits

Kryptografins grunder

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment
Course syllabus for DD2448 valid from Autumn 2020

Grading scale
A, B, C, D, E, FX, F

Education cycle
Second cycle

Main field of study
Computer Science and Engineering

Language of instruction
The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes
After a completed course, the student should be able to
• discuss the following basic concepts in cryptography: symmetric and asymmetric encryption, digital signatures, cryptographic hash functions and strong pseudorandom generators and to give examples of instantiations of each concept
• conduct simple analyses of cryptographic constructions such as cryptosystems and cryptographic protocols
• read analyses performed by others of cryptographic constructions such as cryptosystems and cryptographic protocols and decide if the given analysis can be trusted
• read and understand technical articles in cryptography.

Course contents

Specific prerequisites
Single course students:
SF1604 Linear algebra, SF1625 Calculus in one variable, SF1626 Calculus in several variables, SF1901 Probability theory and statistics, DD1337 Programming, DD1338 Algorithms and Data Structures, DD1352 Algorithms, Data Structures and Complexity, SF1630 Discrete Mathematics or corresponding courses

Examination
• ÖVN1 - Exercise, 7.5 credits, grading scale: A, B, C, D, E, FX, F
Based on recommendation from KTH’s coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Other requirements for final grade
Written exercises (OVN1; 7,5 university credits).

Ethical approach
• All members of a group are responsible for the group’s work.
• In any assessment, every student shall honestly disclose any help received and sources used.
• In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.