DD2520 Applied Cryptography 7.5 credits

Tillämpad kryptografi

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

On 2020-10-13, the Head of the EECS School has decided to establish this official course syllabus to apply from spring semester 2021, registration number J-2020-1831.

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Completed course in computer security equivalent to DD2395.

Active participation in a course offering where the final examination is not yet reported in LADOK is considered equivalent to completion of the course.

Being registered for a course counts as active participation. The term 'final examination' encompasses both the regular examination and the first re-examination.

Language of instruction

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

Intended learning outcomes

After passing the course, the student should be able to:

- use basic terminology in computer security and cryptography correctly
- describe cryptographic concepts and explain their security properties
- find and use documentation of cryptographic libraries and standards
- identify and categorise threats against a cryptographic IT-system at a conceptual level, suggest appropriate countermeasures and present the reasoning to others

in order to

- as citizen and engineer be able to discuss applied cryptography in general, and risks of using/developing cryptography in particular
- in professional life and/or research and development project be able to evaluate challenges in software development related to cryptography.

Course contents

Basic concepts and principles of cryptography, intuition about security, implementation and engineering aspects as well as influence on society, black box analysis, use of cryptographic primitives such as symmetric and asymmetric encryption in applications, digital signatures, cryptographic hash functions and simple crypto systems and cryptographic protocols.

Examination

- INL1 - Assignments, 2.5 credits, grading scale: P, F
- LAB1 - Laboratory work, 5.0 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.

Transitional regulations

The outdated module TEN1 can be examined through compensatory assignments.

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.