DD2520 Applied Cryptography 7.5 credits

Tillämpad kryptografi

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

Establishment

Course syllabus for DD2520 valid from Autumn 2019

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 DD2395 Computer Security 6 credits, or equivalent course.

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 students should be able to:

· use basic terminology in computer security and cryptography correctly,

· describe cryptographic concepts and explain their security properties,

· identify and categorise threats against an IT system at a conceptual level,

· find and use documentation of cryptographic libraries and standards,

· analyse descriptions of cryptographic systems and protocols in terms of black box cryptographic primitives from a software engineering perspective,

· identify vulnerabilities based on system descriptions, estimate the level of threat, suggest countermeasures against identified threats as well as show that they are efficient,

· compare countermeasures, evaluate their side effects and present their 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, intuition about safety, implementation and engineering aspects as well as influence on society, black box analysis, use of cryptographic primitives as symmetric and asymmetric encryption in applications, digital signatures, cryptographic hash functions and simple cryptosystems and cryptographic protocols.

Course literature

Information about the course literature will be announced in the course memo.

Examination

- TEN1 - Written exam, 2.5 credits, grading scale: A, B, C, D, E, FX, 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.

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

The examiner decides, in consultation with KTH's coordinator for disabilities (Funka), about possible adapted examination for students with documented, permanent disabilities. The examiner may permit other examination format for re-examination of individual students.

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.