DD2448 Foundations of Cryptography 7.5 credits

Kryptografins grunder

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

Establishment

The official course syllabus is valid from the spring semester 2022 in accordance with Head of School decision: J-2021-1740. Decision date: 10/08/2021

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Knowledge of algorithms and complexity, 7.5 credits, equivalent to completed course DD2350 / DD2352.

Knowledge of discrete mathematics, 7.5 credits, equivalent to completed course SF1610 / SF1630 / SF1662 / SF1679 / SF1688.

Knowledge in probability theory and statistics, 6 credits, equivalent to completed course SF1912 / SF1914 / SF1915 / SF1916 / SF1920 / SF1921 / SF1922 / SF1923 / SF1924.

Knowledge of algebra and geometry, 7.5 credits, equivalent to completed course SF1624 / SF1672.

Knowledge in one-variable calculus, 7.5 credits, equivalent to completed course SF1625 / SF1673.

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 shall be able to

- discuss the following basic concepts in cryptography: symmetric and asymmetric encryption, digital signatures, cryptographic hash functions, and strong pseudo-random number generator
- give examples of the above concepts
- perform simple own analyzes of cryptographic constructions such as cryptographic systems and cryptographic protocols
- determine the reliability of analyzes of cryptographic constructions such as cryptographic systems and cryptographic protocols
- summarize the content of technical articles on cryptography and cryptographic protocols

in order to be able to work with analysis and development of cryptographic protocols and systems.

Course contents

Classic cryptosystems. What does secure encryption mean? Background in information theory, entropy. Symmetric encryption algorithms such as Advanced Encryption Standard (AES). Open key systems for encryption and digital signatures e.g. RSA, ElGamal and Schnorr signatures. Cryptographically secure hash functions in theory and practice (SHA). Properties and examples of pseudo-random number generators. Connections to complexity theory.

Examination

- GRU1 - Group work, 2.5 credits, grading scale: P, F
- INDA - Individual home assignment, 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.

GRU1 is an investigative group work on a topic described in scientific articles and / or proposed or established standards. It is assessed through a written report and / or oral presentation.

INDA is a set of problems that are solved individually and assessed both in writing and orally.

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.