DD2448 Foundations of Cryptography 7.5 credits

Kryptografins grunder

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

Establishment

Course syllabus for DD2448 valid from Spring 2010

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Single course students: 90 university credits including 45 university credits in Mathematics or Information Technology. English B, or equivalent.

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

Classical encryption methods. What is meant by secure encryption? Background in information theory, entropy. Symmetric encryption algorithms, for example the Advanced Encryption Standard (AES). Public-key cryptosystems 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 between complexity theory and cryptography.

Course literature

Stinson, Cryptography; theory and practice, Chapman & Hall.

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.

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

In this course all the regulations of the code of honor at the School of Computer science and Communication apply, see: http://www.kth.se/csc/student/hederskodex/1.17237?l=en_UK.

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.