



IV1013 Introduction to Computer Security 7.5 credits

Introduktion till datasäkerhet

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 IV1013 valid from Spring 2019

Grading scale

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

Education cycle

First cycle

Main field of study

Technology

Language of instruction

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

Intended learning outcomes

The course gives an introduction to the basics of cryptography, security in computer systems, and network security. On completion of the course the student should be able to:

- explain basic mechanisms in, and the structure of, secure communications protocols
- describe weaknesses in computer systems, software, networks, and communications protocols as well as explain attacks that utilise such weaknesses
- explain and compare advantages and disadvantages with common cryptographic technologies
- design and implement simple cryptographic applications
- account for and recognise threats against information security: confidentiality, integrity, and availability. as well as choose appropriate methods to protect against threats
- design, implement, and evaluate security in networks.

Course contents

- Basic cryptography: symmetric and asymmetric cryptography.
- Cryptographic hashing and digital signatures.
- Security in protocols and services of the Internet.
- Certificates and infrastructures for open key encryption.
- Security in network systems: routers, firewalls, and systems to detect intrusion.
- Security in operating systems.
- Software security: vulnerability, attacks, and defence mechanisms.

Specific prerequisites

- ID1018 Programming I
- IK1203 Networks and communication
- IS1200 Computer Hardware Engineering
- IX1500 Discrete Mathematics

Or equivalent courses.

Course literature

Goodrich, Tamassia: Introduction to Computer Security: Pearson New International Edition - Se vidare: <http://catalogue.pearsoned.co.uk/educator/product/Introduction-to-Computer-Security-Pearson-New-International-Edition/9781292025407.page#sthash.aaLrqfj7.dpuf>

Examination

- INLB - Written Assignment, 1.5 credits, grading scale: P, F

- PRO1 - Project Assignment, 6.0 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.

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.