Cryptology

Programme course

6 credits

Kryptoteknik

TSIT03

Valid from: 2017 Spring semester

Determined by
Board of Studies for Computer Science and Media Technology

Date determined
2017-01-25

Main field of study

Information Technology, Computer Science and Engineering, Computer Science

Course level

Second cycle

Advancement level

A1X

Course offered for

- Computer Science and Engineering, M Sc in Engineering
- Information Technology, M Sc in Engineering
- Computer Science and Software Engineering, M Sc in Engineering
- Industrial Engineering and Management - International, M Sc in Engineering
- Industrial Engineering and Management, M Sc in Engineering
- Applied Physics and Electrical Engineering, M Sc in Engineering
- Communication Systems, Master's programme
- Computer Science, Master's programme
- Mathematics, Master's programme
- Applied Physics and Electrical Engineering - International, M Sc in Engineering

Entry requirements

Note: Admission requirements for non-programme students usually also include admission requirements for the programme and threshold requirements for progression within the programme, or corresponding.

Prerequisites

Algebra and probability theory

Intended learning outcomes

After completing this course the student should be able to make a reasonable assessment of given cryptographic systems and choose a good solution for situations where

cryptographic techniques can help.
Knowledge is required about what basic types of algorithms that exist, what requirements each type must fulfill and how each type works in principle. For some algorithms and algorithm classes, like RSA, Feistel networks etc., also the exact structure must be known.
The student should master the basic principles of cryptanalysis to the extent of being able to systematically apply them to solve simple examples of historical algorithms.
The student is expected to be able to use the general algorithm requirements and algorithm knowledge to perform simple evaluations and point out weaknesses of algorithms and how they are used.

Course content

- Cryptography as a tool for information security, history and principles.
- Theoretic foundations.
- Perfect systems and randomness.
- Stream ciphers.
- Pseudorandom sequences and their connection to the theory for linear and non-linear feedback shift registers.
- Principles for and examples of symmetric block ciphers.
- Public key encryption and public key distribution.
- Crypto based checksums, cryptographically strong hash functions and digital signatures.
- Quantum cryptography.
- Zero knowledge.
- Protocols and algorithms for current applications, which illustrate the use of advanced cryptographic techniques.

Teaching and working methods

The course consists of lectures, problem solving sessions and two laboratory assignments.

Examination

LAB1	Laboratory work	U, G	2 credits
TEN2	Written examination	U, 3, 4, 5	4 credits

The laboratory assignment consists of two sets of problems to solve with the help of computers.

Grades

Four-grade scale, LiU, U, 3, 4, 5

Department

Institutionen för systemteknik

Director of Studies or equivalent

Klas Nordberg

Examiner

Jan-Åke Larsson

Course website and other links

http://www.icg.isy.liu.se/courses/tsit03

Education components

Preliminary scheduled hours: 34 h
Recommended self-study hours: 126 h

Course literature

Additional literature

Books

Trappe, Washington, (2006) *Introduction to Cryptography with Coding Theory* Prentice Hall

Common rules

Regulations (apply to LiU in its entirety)

The university is a government agency whose operations are regulated by legislation and ordinances, which include the Higher Education Act and the Higher Education Ordinance. In addition to legislation and ordinances, operations are subject to several policy documents. The Linköping University rule book collects currently valid decisions of a regulatory nature taken by the university board, the vice-chancellor and faculty/department boards.

LiU's rule book for education at first-cycle and second-cycle levels is available at http://styrdokument.liu.se/Regelsamling/Innehall/Utbildning_pa_grund-_och_avancerad_niva.