LUNDS UNIVERSITET
Lunds Tekniska Högskola

Course syllabus

Kryptoteknik
Cryptography

EDIN01, 7,5 credits, A (Second Cycle)

Valid for: 2023/24
Faculty: Faculty of Engineering, LTH
Decided by: PLED C/D
Date of Decision: 2023-04-18

General Information

Elective for: C4-ks, C4-sec, D4-ns, E4-ks, F4, MSOC1, MWIR2, Pi4-pv, MMSR2
Language of instruction: The course will be given in English on demand

Aim

This course is intended to be an introduction to the fascinating subject of cryptography. It provides both a firm ground in the fundamentals and a feel for the subject for anyone interested either in carrying out cryptographic research or employing cryptographic security.

Learning outcomes

Knowledge and understanding
For a passing grade the student must

- be able to describe different building blocks used in cryptology,
- be able to describe the general problems that are addressed by cryptology,
- be able to explain the principles behind different cryptographic primitives.

Competences and skills
For a passing grade the student must

- be able to identify and formulate problems in the area of cryptology
- be able to provide descriptions of how cryptographic primitives can be used in security systems.
- be able to show that you are capable to choose suitable parameters to cryptographic primitives as well as analyze various constructions from a security perspective.

During the course you have to present and discuss your knowledge through exercises and several smaller mandatory projects.

Contents

Classical cryptography: Introduction and basic notation, The Caesar cipher, simple substitution, polyalphabetic ciphers (Vigenére, Kasiski's method, Vernam), transposition ciphers, rotor machines (Enigma).

Shannon's theory of secrecy: entropy, key and message equivocation, redundancy, unicity distance, perfect secrecy.

Shift register theory and stream ciphers: Finite fields, linear feedback shift register sequences, periods and cycle sets, shift register synthesis, nonlinear combinations of sequences, attacks on stream ciphers.

Block ciphers: Data Encryption Standard (DES), Advanced Encryption Standard (AES).

Public key cryptography: Basic number theory, RSA, Diffie-Hellman key exchange, factoring, primality, digital signatures.

Hash functions: properties, collision attacks, the birthday paradox

Authentication codes: Impersonation and substitution attacks.

S*ecret sharing*: Shamir's threshold scheme, general secret sharing, perfect and ideal schemes.

Projects: 1. Factoring. . 2. Shift register sequences. 3. Correlation attacks

Examination details

Grading scale: TH - (U,3,4,5) - (Fail, Three, Four, Five)
Assessment: Written exam and three mandatory projects.

The examiner, in consultation with Disability Support Services, may deviate from the regular form of examination in order to provide a permanently disabled student with a form of examination equivalent to that of a student without a disability.

Parts
Code: 0118. **Name:** Examination.
Credits: 4,5. **Grading scale:** TH. **Assessment:** Written exam. **Contents:** The whole course-
Code: 0218. **Name:** Projects.
Credits: 3. **Grading scale:** UG. **Assessment:** Approved projects. **Contents:** The course has three mandatory projects covering different parts of the course.

Admission

Assumed prior knowledge: A first course in programming. Basic mathemathics like linear algebra and probability theory.
The number of participants is limited to: No
The course overlaps following course/s: EDI051

Reading list

- Lecture notes in cryptology (distributed by the department).
- Alternative literature: Stinson, D., Cryptography, Theory and Practice, CRC Press, ISBN 1-58488-206-9 or Smart, N., Cryptography: An Introduction, McGraw-Hill, ISBN 0077099877.

Contact and other information

Course coordinator: Professor Thomas Johansson, thomas@eit.lth.se
Course homepage: http://www.eit.lth.se/course/edin01