LUNDS UNIVERSITET
Lunds Tekniska Högskola

Course syllabus

Avancerad kryptografi
Advanced Cryptography

ETIN85, 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-sec, D4-ns, E4, F4, MSOC2, MWIR2, Pi4
Language of instruction: The course will be given in English

Aim

The purpose of the course is to show how advanced algorithms and protocols in cryptology work and that they have great practical applications in data security.

Learning outcomes

Knowledge and understanding
For a passing grade the student must

- describe the definition and function of a number of advanced primitives and protocols in cryptology that are covered in the course.
- explain mathematical principles behind advanced cryptographic building blocks.
- describe models for security and proofs for cryptographic primitives.

Competences and skills
For a passing grade the student must

- identify and formulate mathematical problems relevant to advanced algorithms in cryptology.
- mathematically analyse different possible constructions from a security perspective.
- implement relevant primitives or attacks for simulation

Judgement and approach
For a passing grade the student must

- be able to independently classify how different primitives and their parameters are linked to different models and levels in security.

Contents

In terms of content, the course provides a number of advanced tools in cryptology that have many applications in data security. Most of the systems covered in the course are used in various communication systems, for example cryptosystems constructed via elliptic curves. We treat the mathematical background needed to be able to understand how such systems work. We also look at how to mathematically prove that systems or protocols are secure and the models that exist.

More specifically, we deal with most of the following areas: Discrete logarithms and their cryptosystems; Elliptic curves and their cryptosystems; Factoring and discrete log problems; Advanced types of symmetric cryptosystems, digital signatures and hash functions, authentication and secret sharing; Complexity theory, Provable security, Random-oracle model; MPC primitives and homomorphic encryption; Post-quantum cryptology.

Examination details

Grading scale: TH - (U,3,4,5) - (Fail, Three, Four, Five)
Assessment: To pass the course, approved projects and home assignments are required. In addition to this, an approved written exam is required, where the result gives the grade in the course. Approved home assignments are a requirement for writing the exam.

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: 0121. **Name:** Project.
Credits: 3. **Grading scale:** UG. **Assessment:** Approved projects and home assignments.
Code: 0221. **Name:** Examination.
Credits: 4,5. **Grading scale:** TH. **Assessment:** Written exam.

Admission

Admission requirements:

- EDI051 Cryptography or EDIN01 Cryptography

The number of participants is limited to: No
The course overlaps following course/s: EDIN05

Reading list

- Nigel Smart: Cryptography Made Simple, (Information Security and Cryptography). Springer, 2016, ISBN: 978-3319219356.

Contact and other information

Course coordinator: Thomas Johansson, thomas@eit.lth.se