DALARNA UNIVERSITY

Course Syllabus

Cryptography 7.5 Credits*, First Cycle

Learning Outcomes

Upon completion of the course the student shall be able to:

- Explain cryptographic concepts
- Compare symmetric and asymmetric encryption methods
- Apply hash algorithms within digital forensic situations and for authentication
- Carry out simpler types of cryptanalytic attack
- Integrate cryptographic components into software in a secure manner
- Apply block chain technology to solutions
- Judge the cryptographic strength of a system
- Evaluate the societal role of cryptography from a social, ethical and economic standpoint

Course Content

The course starts with a historical introduction to cryptography, Kerchoff´s principle and the pioneering work of Shannon and Feistel, who established the foundation for symmetric block ciphers. Following this, symmetric encryption is explored, with a focus on standards such as DES, 3DES, AES and the other contenders. Symmetric encryption is extended to yield either a stream cipher or a random number generator for key production. Drawbacks of symmetric encryption are discussed, with a focus on the key distribution problem. Asymmetric encryption is introduced as a solution to the key distribution problem, with a focus on the Diffie-Hellman and RSA algorithms. Asymmetric cryptography is applied to the issue of message authentication. Combined symmetric and asymmetric encryption is introduced as espoused by the PGP architecture. Hashing algorithms are explored, with a focus on applications in digital forensics. Cryptanalysis is discussed, including brute force attacks, differential and linear cryptanalysis and side-channel attacks. Different cryptanalytic situations are defined with respect to quantity and type of empirical data available. Blockchains and digital currencies are introduced.

Assessment

A written home examination that the student must discuss/present for a grade 5 credits, laboratory reports 2.5 credits.

DALARNA UNIVERSITY

Forms of Study
Lectures and laboratory work

Grades
The Swedish grades U–VG.

To pass the course, the student must pass the laboratory reports and the home examination. The grade for the entire course is determined by the examination grade, provided that the student receives a passing grade for laboratory reports.

Prerequisites
Fundamentals of programming 7,5 credits

Other Information
Replaces DT2017.

Subject:
Microdata Analysis

Group of Subjects:
Other Interdisciplinary Studies

Disciplinary Domain:
Natural Science, 100%

This course can be included in the following main field(s) of study:
1. Microdata Analysis

Progression Indicator within (each) main field of study:
1. G1F

Approved:
Approved 21 February 2019
Valid from 6 May 2019