Course information

EDIN01 - CRYPTOLOGY

Department of EIT
Lund University

Reading period ht2, 2020

Credits: 7.5 hp.

Course lecturer/examiner: Thomas Johansson

`http://www.eit.lth.se`

The purpose of the course is to give a summary of classical cryptosystems and then a more thorough treatment of some aspects in modern cryptology.

Cryptology is the science of mathematical methods of securing communication and information systems. Such systems have traditionally been used by military officers, diplomats and spies for a few thousand years. In recent time, civilian need for data protection has increased most significantly. This is mainly due to advances in computer and communication technology, which has enabled the rapid collection, processing and distribution of huge amounts of datasets. Geographically dispersed banks, industries and authorities are now totally dependent on electronic devices information transfer. They all need to secure their information, transmitted or stored and cryptology offers the building blocks to do so.

CONTENTS

Introduction. Introduction and basic concepts.

Classical cryptosystems. Caesar cipher, simple substitution, polyalfabetic ciphers, (Vigenére, Kasiski's method, Vernam), transposition, (Hagelin M-209).

Shannons theory of secrecy. Some concepts in discrete probability theory, Shannon's theory of secrecy.

Stream Cipher and Shift Register Sequences. Finite fields and linear feedback shift registers and their sequences, periods and cycle sets, shift registers synthesis, functions of shift register sequences, randomness characteristics. Analysis of the stream cipher and possible attacks.

Block ciphers. Feistel ciphers and SPN networks. Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Modes of operation.

Basic number theory. Basic Number theory, primality, factorization and exponentiation.

Public-key cryptosystems. Introduction to public-key cryptosystems, the RSA-system, Diffie-Hellman key distribution, Digital signatures.

Hash functions. design and analysis, birthday paradox.

Message authentication. authentication codes and MACs.

Secret Sharing Schemes. Shamir Threshold Scheme, general access structures.

LITERATURE

Lecture notes (in English) will be available for printing on the course website. The same applies to the project descriptions. In addition, we recommend the following books as supplement:

D. Stinson, *Cryptography, Theory and Practice*, third edition, ISBN 1-58488-508-4.

N. Smart, *Cryptography, An Introduction*, ISBN 0077099877. (available in full text on the web), or
N. Smart, *Cryptography Made Simple*, Springer International Publishing, 2015. ISBN: 978-3-319-04041-7.

A few copies of each book are available in the E-house library (?).

TEACHING

Lectures (36 hours, week 1–7): Thomas Johansson

Tuesday	15-17	ZOOM
Wednesday	10-12	ZOOM
Thursday	08-10	ZOOM

Three occasions will be cancelled!

Exercise hours (14 hours, week 1–7): Qian Guo

Group 1	Friday	10-12	ZOOM

Mandatory projects: Qian Guo

1. *Factoring algorithms* – week 2–3.
2. *Shift register sequences* – week 3–4.
3. *Correlation attacks* – week 4–5.

Information on the implementation of the projects is available on the course website. Note that some lectures are preparing projects!

COURSE WEBPAGE

`http://www.eit.lth.se/` and onwards.
It contains all information about the course, here you can download documents, etc.

EXAM

Written exam (5 hours) of problem solving type. (fail, grade 3-5). Ordinary exam: 2021-01-11 14:00–19:00 in ??. Please note that approved projects is a requirement to be allowed to take the exam.