HI117V IT-Security I 7.5 credits

IT-säkerhet I

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for HI117V valid from Autumn 2008

Grading scale

A, B, C, D, E, FX, F

Education cycle

First cycle

Main field of study

Electrical Engineering,Technology

Specific prerequisites

Completed upper secondary education incl documented proficiency in English.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After the project course the student should know:

• The principles of IT-Security and Cryptology

Course contents

The course consists of the following topics:

Overview; Classical Encryption Techniques, Block Ciphers and the Data Encryptions Standard; Introduction to Finite Fields, Advanced Encryption Standard; Contemporary Symmetric Ciphers; Confidentiality using Symmetric Encryption; Introduction to Number Theory; Public-Key Cryptography; Message Authentication and Hash Functions; Hash and Mac Algorithms; Digital Signatures and Authentication Protocols; Authentication Applications; Electronic Mail Security; IP Security; Web Security; Intruders and Viruses; Firewalls; Standards and Standard-setting Organizations; Project for Teaching Cryptography and Network Security.

Disposition

Course disposition: The course is given in English and is of half time studies. The course is a distance course. For further information in English, please contact the teacher.

Course literature

Computer Security: Principles and Practice;

William Stallings, Lawrie Brown; 2008, 880 pp. Prentice Hall;

ISBN-10: 0136004245

ISBN-13: 9780136004240

Classical and Contemporary Cryptology;

Richard J. Spillman 2004, 304 pp

Prentice Hall,

ISBN-10: 0131828312

ISBN-13: 978-0131828315

/This book is included in the Digital Course Notes, with author´s permission/

Digital Course Notes IT-Sec I, 3 CDs, 1.5 GB, L.O. Stromberg

Equipment

You will need:

* A personal computer (PC) running Windows XP/ Vista/ 7

* Internet access

* two working email addresses (do not use free webmail clients, use POP3)

* A scientific pocket calculator

Examination

- ANN1 - Assignment, 1.5 credits, grading scale: P, F
- ANN2 - Assignment, 1.5 credits, grading scale: P, F
- ANN3 - Assignment, 1.5 credits, grading scale: P, F
- TEN1 - Examination, 3.0 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Examinations are offered three times a year: typically the first Saturday in May, August, and December.

Written examinations are four hours long, and consist of 68 questions; 60 of which are multiple choice (5 choices each) and 8 are in depth questions, including mathematical calculations. The Final examination in IT-Sec III is a lab project.

Written examinations worldwide can usually be arranged at other universities, as well as at Swedish embassies and consulates.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.