IMT3771 Introduction to Cryptology - 2012-2013

Emnekode:
IMT3771

Emnenavn:
Introduction to Cryptology

Faglig nivå:
Bachelor (syklus 1)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
First half of the autumn semester

Språk:
Engelsk

Forventet læringsutbytte:
Knowledge

The candidate possesses broad knowledge about main topics and theories in cryptology, its processes, tools and methods. The main topics and theories include classical cryptography, symmetric ciphers, asymmetric ciphers, hash functions and digital signatures.

The candidate is familiar with research and development achievements in modern cryptology.

The candidate is capable of updating his/her knowledge in cryptology.

Skills

The candidate is capable of applying the knowledge in cryptology and the relevant research and development results to theoretical and practical problems. The candidate is also capable of giving the explanation for the choice of those results applicable on the problem at hand.

The candidate is capable of thinking over his/her professional practice and making changes in it under supervision.

The candidate can find, evaluate and refer to relevant research results and other achievements in cryptology and use them to solve a particular problem.

The candidate knows relevant cryptographic tools techniques and terminology.

General competence

The candidate has insight into relevant professional and ethical problems.

The candidate is capable of planning and carrying out various professional tasks and projects during certain time period, alone or as a member of a group, following ethical requirements and guidelines.

The candidate can communicate the most important material in cryptology such as theories, problems and solutions through written, oral and other relevant forms of expression.

The candidate can exchange points of view and experience with others possessing background in cryptology. Through that process, the candidate can contribute to development of good practice.

The candidate possesses knowledge about innovation and innovation processes.

Emnets temaer:
1. Classical cryptography - history of cryptography and classical cipher systems

2. Symmetric ciphers - introduction to stream and block ciphers

3. Asymmetric ciphers - definition and fundamentals

4. Hash functions and digital signatures.

Pedagogiske metoder:
Forelesninger
Oppgaveløsning

Pedagogiske metoder (fritekst):
Lectures

Numerical exercises

The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC’s learning management system (ClassFronter).

Vurderingsformer:
Skriftlig eksamen, 3 timer

Vurderingsformer:
Written exam, 3 hours

Karakterskala:
Bokstavkarakterer, A (best) - F (ikke bestått)

Sensorordning:
Evaluated by internal examiner, external examiner is used periodically (every four years, next time in 2012/2013)

Utsatt eksamen (tidl. kontinuasjon):
Ordinary re-sit examination.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Calculator, dictionary

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
Books:

1. Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.

Erstatter:
IMT3701 Cryptology

Supplerende opplysninger:
There is room for 50 students for the course.

Klar for publisering:
Ja

Emneside (URL):
http://www.hig.no/imt/emnesider/imt4532