IMT4532 Cryptology 1 - 2016-2017

Emnekode:
IMT4532

Emnenavn:
Cryptology 1

Faglig nivå:
Master (syklus 2)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
First half of the fall semester

Språk:
Engelsk

Forventet læringsutbytte:
Knowledge

- The candidate possesses advanced knowledge of classical cryptography, as well as of stream ciphers, block ciphers and public key ciphers.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for cryptology.
- The candidate is capable of applying his/her knowledge in new fields of cryptology.

Skills

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of cryptology and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in cryptology.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in cryptology.
- The candidate is capable of carrying out an independent limited research or development project in cryptology under supervision, following the applicable ethical rules.

General competence

- The candidate is capable of analyzing relevant professional and research ethical problems in cryptology.
- The candidate is capable of applying his/her cryptographic knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with cryptographic terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of cryptology, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

Emnets temaer:
1. Classical cryptography - history of cryptography, fundamentals of information theory and its application in cryptography

2. Symmetric ciphers - stream and block ciphers

3. Asymmetric ciphers - fundamentals, RSA

4. Hash functions and digital signatures.

Pedagogiske metoder:
Forelesninger
Oppgaveløsning
Prosjektarbeid

Pedagogiske metoder (fritekst):
Lectures

Numerical exercises

The course will be made accessible to 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).

Project work

Vurderingsformer:
Skriftlig eksamen, 3 timer
Vurdering av prosjekt(er)

Vurderingsformer:
Written exam, 3 hours, counts for 70% of the final mark

Project, counts for 30% of the final mark

Both the exam and the project must be passed

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

Sensorordning:
Evaluated by the lecturer. An external examiner will be used every 4th year. Next time in the school-year 2018/2019.

Utsatt eksamen (tidl. kontinuasjon):
Re-sit examination for the written exam in August. The project work (if passed) need not be repeated.

Tillatte hjelpemidler:
D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.

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

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig kobling:
Slobodan Petrovic

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
Books:

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

2. Handbook of Applied Cryptography, Menezes A., http://www.cacr.math.uwaterloo.ca/hac

Erstatter:
IMT4531 Introduction to Cryptology

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

The students that have already taken the course IMT3771 "Introduction to cryptology" at the bachelor level and that continue with the master's program in information security at HiG cannot be exempted from taking the course IMT4532 Cryptology 1 on the master's level since the expected learning outcomes and the evaluation methods in these two courses are different (the written exam is different and there is a compulsory project in IMT4532).

Klar for publisering:
Ja