Faculty of Health, Science and Technology

Doctoral Course

Curriculum Approval

The syllabys was approved by the board of the Faculty of Health, Science and Technology on 30 September 2015 (Dnr HNT 2015/152), valid as of Spring 2016.

Doctoral discipline/field

Computer Science

Course name (English)

Topics in Cryptography

Credit

3 hp/ECTS

Language of instruction

English

Education level

PhD education

Target audience and admission requirements

This course is for PhD students in Computer Science or related subjects.

Learning outcomes

Cryptography is a basic building block for secure and privacy-enhancing technologies. This course will give an introduction into advanced cryptographic schemes and their applications for building secure and privacy-enhancing technologies and will study and discuss current research topics in applied cryptography.

After the course, the students should be able to:

- understand and explain advanced crypto concepts and be able to use them correctly;
- understand different current research topics and research challenges in cryptography;
- analyse the security of cryptographic protocols and understand the challenges of designing secure crypto protocols;

such that the students can:

- reason about the strength and limitations of cryptographic schemes;
- select suitable cryptographic functions for achieving security and privacy by design and
- incorporate existing crypto schemes or protocols into their research projects or develop new or enhanced crypto solutions.

Course content

The course consists of four full-days with lectures and exercises to be solved in the class or afterwards. After the four days of block lectures and exercises, the attendees will be assigned or can choose a related applied crypto paper that they have to study and then present and discuss in the class and explain to the examiner.

Course content/schedule:

1) General introduction
2) Symmetric key crypto foundations: Stream ciphers (brief), block ciphers (DES, 3DES, AES, modes of operation), hash functions (password hashing, birthday paradox, MD construction, sponge constructions, MD5, SHA1, SHA2, SHA3), MAC (CMAC, HMAC)
3) Public key crypto foundations: Diffie-Hellman, RSA, ElGamal, Zero-knowledge proofs, signatures
4) Advanced schemes and concepts: Authenticated encryption (also composition MAC and ENC), Key establishment (SIGMA-I), ECC, key lengths, PKI
5) Crypto protocol design
6) Towards functional signatures: Blind signatures, Partially blind signatures, High level overview of functional and malleable signatures
7) Secret sharing: Homomorphic encryption, signatures, High level Multiparty computation, High level homomorphic encryption, fully homomorphic encryption
8) High-level quantum cryptography

Course reading and other study resources

The course literature consists of a reading list of selected research papers. The current reading list that is published below may be amended as the course proceeds.

Examination

To pass the course, the students successfully complete the following tasks:

- Attend at least 80% of the lectures
- Complete the exercises
- Select a related crypto research paper and present and explain it in the class

Certificate of course completion

Will be issued upon request of the PhD student.

Quality control

The course will be evaluated in oral and written form during and after the course. The evaluation will be summarized and reported by the teachers according to Högskoleförordningen 1 kap. 14 §.

Grade

The grading is pass (godkänd - G) or fail (underkänd - U).

Course literature

The course literature consists of selected research papers:

- Daniel J. Bernstein and Tanja Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography*. http://safecurves.cr.yp.to 2015.
- Hugo Krawczyk: SIGMA: *The 'SIGn-and-MAc' approach to authenticated Diffie-Hellman and its use in the IKE-protocols*. CRYPTO 2003.
- Daniel J. Bernstein: *Introduction to post-quantum cryptography*. Post-quantum cryptography 2009.
- Nikita Borisov, Ian Goldberg, Eric A. Brewer: *Off-the-record communication, or, why not to use PGP*. WPES 2004.
- Daniel J. Bernstein, Tanja Lange and Peter Schwabe: *The security impact of a new cryptographic library*. LatinCrypt 2012.
- Dan Boneh, Matthew K. Franklin: *Identity-Based Encryption from the Weil Pairing*. CRYPTO 2001.