Tárgyleírás angol nyelvű képzés tárgya esetén

Tárgy neve: Post-quantum cryptography L.

Tárgyfelelős neve: Kutas Péter

Tárgyfelelős tudományos fokozata: PhD

Tárgyfelelős MAB szerinti akkreditációs státusza: AT

Az oktatás célja angolul / Aim of the subject:

Knowledge

- In order to be able to perform their work in an innovative way and do research (when necessary) in their own IT specialisation, they have comprehensive and up-to-date knowledge of general mathematical and computing principles, rules and relationships, particularly in the following areas: algebraic, linear algebraic and number theory methods and applications; algorithmic methods in mathematics, formal models and tools in computing science, complexity and efficiency theory of algorithms, and special algorithms of application fields.
- They have comprehensive and up-to-date knowledge and understanding of the general theories, contexts, facts, and the related concepts of IT, particularly in the areas of computer networks, information theory, cryptography.
- They have comprehensive and up-to-date knowledge of the principles, methods, and procedures for designing, developing, operating, and controlling IT processes, particularly in the areas of the design, construction and management of cryptography, data security and data protection.
- They have a high level of fluency in the language of IT – including its professional vocabulary and its characteristic features of expression and composition – both in their mother tongue and in English, at least.

Abilities:

- They are able to apply their mathematical, computer science and informatics skills in a novel way in order to solve tasks in IT research and development.
- They are able to formalize complex IT tasks, to identify and study their theoretical and practical background and then to solve them.
- They are able to initiate collaboration and work in a team as well as on projects with IT or other professionals.
- They are able to professionally use scientific and technical information sources to obtain knowledge necessary for solving a problem, and to critically interpret and evaluate it.

Attitude:

- They follow professional and technological developments in their IT field.
- They share their knowledge and consider it important to disseminate professional IT results.

Autonomy, responsibility:

- They take responsibility for their professional decisions made in their IT-related activities.

Az oktatás tartalma angolul / Major topics:

The main goal of this course is to give a detailed overview of the mathematical background behind recent post-quantum algorithms including the novel computational hardness assumptions and the related cryptographic protocols. The course also introduces several NIST winners and finalists. The course covers topics from:

- Breaking discrete log and factoring with the hidden subgroup problem
- basics of lattices and hard lattice problems (SVP, CVP)
- lattice reduction algorithms (Babai's nearest plane alg, LLL)
- ideal lattices, NTRU
- Ring-LWE and Module-LWE problems
- multivariate cryptography, HFE and Oil and Vinegar schemes
- elliptic curves and isogenies and protocols (CSIDH, SQISign, ...)
- Error-correcting codes. The McEliece cryptosystem and attacks

A számonkérés és értékelés rendszere angolul / Requirements and evaluation:

exam

Irodalom / Literature:

- D.J. Bernstein, J. Buchmann, E. Dahmen: Post-Quantum Cryptography, Springer, 2009, ISBN: 978-3-540-88701-0
- L. De Feo: Mathematics of Isogeny Based Cryptography, 2017, https://arxiv.org/abs/1711.04062