Tárgy neve: Cryptography

Tárgyfelelős neve: Ligeti Péter

Tárgyfelelős tudományos fokozata: PhD, egyetemi docens

Tárgyfelelős MAB szerinti akkreditációs státusza: AT

Az oktatás célja angolul:

a) knowledge

- They have comprehensive and up-to-date knowledge and understanding of the general theories, contexts, facts, and the related concepts of IT, particularly – depending on their chosen specialization – in the areas of program design, synthesis and verification, logical programming, programming languages, computing models, computer architectures, operating systems, computer networks, distributed systems, database management systems, information theory, code theory, and cryptography.
- They have comprehensive and up-to-date knowledge of the principles, methods, and problem solving approaches of the IT domain that contains processes for designing, developing, operating, and controlling of IT Systems, particularly – depending on their chosen specialization – in the areas of programming technology; design, construction and management of complex software systems and state-of-the-art databases; service-oriented program design; the design, construction and management of information systems; the design and development of internet tools and services; the design, development and management of database systems; the design, construction and management of distributed systems, cryptography, data security and data protection.

b) skills and abilities

- They are able to analyze and apply new problem-solving methods and procedures related to their IT specialization
- 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 professionally use scientific and technical information sources to obtain knowledge necessary for solving a problem, and to critically interpret and evaluate it.
- Under professional guidance, they are able to carry out scientific research on their own, and to prepare for further studies at postgraduate level.

c) attitude

- They follow professional and technological developments in their IT field.
- They are committed to critical feedback and evaluation based on self-examination.
- They are committed to lifelong learning and they are open to acquiring new IT competencies.
- They accept and make their co-workers apply the ethical principles of work and organizational culture as well as those of IT scientific research.
- They share their knowledge and consider it important to disseminate professional IT results.
- They consider it important to propagate and realize environmentally conscious behavior and social responsibility, and they promote them with the help of information technology.
- They are committed to having quality requirements met and to analyzing them with IT tools.
- They are open to proactive collaboration with IT and other professionals.

d) autonomy and responsibility

- They take responsibility for their professional decisions made in their IT-related activities.
- They undertake to meet deadlines and to have deadlines met.

- They bear responsibility for their own work as well as for the work of their colleagues they work together with in a project.
- Regarding mission critical IT systems, they can be entrusted with developing and operational responsibilities that are in accordance with their professional competencies.

Az oktatás tartalma angolul:

The course covers introductory topics in cryptography.. The following concepts are introduced: perfect and computational security, hardness assumptions, provable security. The basic cryptographic primitives covered are

- Symmetric Cryptography
  - pseudo randomness
  - MACs and cryptographic hash functions
  - block and stream ciphers
- Public key cryptography
  - key exchange protocols
  - public key encryption
  - digital signatures

The practical assignments help the students to develop a deeper understanding of cryptographic primitives and understand pitfalls and fallacies.

A számonkérés és értékelés rendszere angolul:

practical course mark and examination

Idegen nyelven történő indítás esetén az adott idegen nyelvű irodalom:

- Jonathan Katz, Yehuda Lindell: Introduction to Modern Cryptography. Chapman & Hall/Crc Cryptography and Network Security Series, 2007. ISBN: 1584885513
- Goldreich, Oded: Foundations of Cryptography, Volume 1, Basic Tools, ISBN 0-521-79172-3 Cambridge University Press, 2001.
- Boneh, Dan and Shoup, Victor: A Graduate Course in Applied Cryptography, preprint, v0.4, https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf
- Various further parts from the literature