I004	FIN-elective–Year 2 MR-obligatory–Semester 3 IPM-elective–Year 2	**Cryptography and System Security**	L+P+S 2+2+0	ECTS 6

Course objectives. The goal of this course is to acquaint students with fundamental terminology and methods of cryptography and security of computer systems. The basic ideas of data encryption and decryption will be presented to students and they will be familiarized with multiuser and multitasking operating systems. Introduction and treatment of notions from the field of cryptography will be presented in lectures with respect to their properties, advantages and disadvantages. Students will be acquainted with encryption and decryption methods by programming and master the techniques of operating systems and database security analysis.

Course prerequisites. Undergraduate study programme in mathematics.

Syllabus.

1. Cryptography. Congruencies in cryptography. Basic properties of congruencies. Euler's theorem, prime and pseudo-prime numbers. Modeling, engineering and validation of security protocols.
2. Data encryption and decryption. Cryptosystems. RSA cryptosystem. Cryptosystems with public keys. Pseudo-random number generation.
3. Authentication. Digital signature. Infrastructure of public key and security control.
4. Security control and monitoring models. Model analysis and unreliable points in the system.
5. Protection. Multilevel secure databases. Network security and safeguard measures. Firewalls and delegate servers.

Expected learning outcomes.

After completing the course, students are expected to:

- demonstrate the knowledge and intelligence as the basis for the original work and development of ideas;
- apply their knowledge, understanding and ability to problem solving in a wider context in the area of cryptography;
- be capable of integrating new knowledge in the area of cryptography;
- be able to communicate their conclusions and supporting arguments to both experts and non-experts;
- possess the learning ability for continuing education and lifelong learning in this area.

Teaching methods and student assessment. Lectures and exercises are obligatory. The final exam consists of a written and an oral part, and it is taken after the successful completion of lectures and exercises. Successful participation in mid-term exams (or homework) replaces obligatory participation in the practical part of the exam. Students can influence their final grade by writing homework and seminar papers.

Can the course be taught in English: Yes.

Basic literature:

1. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 2001. (available on-line)
2. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, 1994.

Recommended literature:

1. D.R. Stinson, Cryptography. Theory and Practice, CRC Press, Boca Raton, 2002.
2. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Codes in C, John Wiley & Sons Inc. 1995.
3. B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons Inc. 2000.