MI003	**Cryptography and System Security**	L	P	S	ECTS
		2	2	0	5

Course objectives. The aim of this course is to introduce students to fundamental concepts and methods of classical and modern cryptography. Students will be introduced to the basic ideas of encryption and decryption of the data, with particular emphasis on applications of the number theory in modern cryptography. Properties of cryptosystems will be studied, methods of protecting operating systems will be introduced, and their advantages and disadvantages will be determined. Students will learn the main decryption methods for particular type attacks on well-known cryptosystems. Variety of encryption and decryption procedures will be introduced, students will make the corresponding programs and test methods on different examples.

Prerequisites. Undergraduate mathematics or computer science study programme.

Course content.

1. Cryptography. Fundamental concepts and attack types. Types of cryptosystems. Classical cryptography and frequency analysis.
2. Congruences in cryptography. Basic properties of congruences, primes and pseudoprimes. Modeling, projecting and testing of the security protocols.
3. Public key criptography. RSA cryptosystem. Generating of the pseudorandom numbers.
4. Authentication. Digital signature. Public key infrastructure and protective management.
5. Secutiry management and monitoring models. Analysis of models and unreliable places in systems.
6. Protection. Multilevel secutiry databeses. Safety dams and representative serves.

LEARNING OUTCOMES

No.	LEARNING OUTCOMES
1.	Differ the types of cryptosystems and the attack types.
2.	Apply the properites of primes and pseudoprimes in the construction of cryptosystems.
3.	Use the public key cryptosystems.
4.	Understand and apply the digital signature procedure.
5.	Identificate the unreliable places in systems.
6.	Analyse the security measures and the procedure of system protection.

RELATING THE LEARNING OUTCOMES, ORGANIZATION OF THE EDUCATIONAL PROCESS AND ASSESSMENT OF THE LEARNING OUTCOMES

TEACHING ACTIVITY	ECTS	LEARNING OUTCOME **	STUDENT ACTIVITY*	EVALUATION METHOD	POINTS	
					min	max
Attending lectures and exercises	1	1-6	The presence at lectures, discussions, teamwork and independent work on assignments	Attendance lists, tracking activities	0	4

Written exam (Mid-terms)	2	1-6	Preparing for the written exam	Verification of correct answers (evaluation)	25	48
Final exam	2	1-6	Revising	Oral exam	25	48
TOTAL	5				50	100

Teaching methods and knowledge assessment. Attendance at lectures and exercises is required. The exam consists of written and oral part, and can be taken after completion of lectures and exercises. During the semester students can take colloquiums that replace the written examination. During the semester students can make a seminar. A well designed seminar affects the final course grade.

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 (dostupno 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, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons Inc., 2000
3. A. Dujella, M. Maretić: Kriptografija, Element, Zagreb, 2007