MI006	**Cryptography**	L	P	S	ECTS
		2	2	0	6

Course objectives. The goal of this course is to acquaint students with fundamental terminology and methods of cryptography and cryptanalysis of different types of cryptosystems. The basic ideas of data encryption and decryption will be presented to students through the modern symmetric and asymmetric cryptosystems. Since the modern cryptosystems are based on the number theory functions, all the necessary basic concepts will be introduced to all necessary places. In that way, it will be easier to study all advantages and disadvantages of different types of cryptosystems.

Prerequisites. Undergraduate university study programme of mathematics and/or computer science.

Course content.

1. Basic concepts. Cryptosystems classification. Attacks to cryptosystems.
2. Substitution ciphers. Caesar cipher. Affine cipher. Letter frequency analysis. Keyword Caesar cipher. Vigenere cipher. Playfair cipher. Hill cipher.
3. Transposition cipher. Permutation cipher. Columnar transposition cipher.
4. Primality tests and some factorization methods. Distribution of primes. Pseudoprimes. Fermat factorization method. Pollard factorization method. Continued fraction factorization method.
5. Public key cryptography. RSA cryptosystem and some of its modifications. Rabin cryptosystem. ElGamal cryptosystem.

LEARNING OUTCOMES

No.	LEARNING OUTCOMES
1.	Distinguish basic types of cryptosystems and their attacks.
2.	Successfully apply the procedure of encrypting and decrypting data in the presented cryptosystems.
3.	Understand the importance of the basic number theory tools in cryptography.
4.	Recognize the role of primes and pseudoprimes in the construction of cryptosystems.
5.	Understand the using of public key cryptosystems.
6.	Successfully apply the presented material in independent solving of homework and mid-terms.

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	Lecture attendance, discussion, independent work on given tasks	Attendance lists, tracking activities	0	4
Homework assignments	1	1-6	Independent work on given problems	Evaluation	0	4

Written exam (Mid-terms)	2	1-6	Preparing for written exam	Evaluation	25	46
Final exam	2	1-6	Revision	Oral exam	25	46
TOTAL	6				50	100

Teaching methods and student assessment. Lectures and exercises are obligatory. The exam consists of a written and an oral part. Upon completion of the course, students can take the exam. Successful midterm exam scores replace the written exam. Students can improve their grades by writing homework assignments.

Can the course be taught in English: Yes

Basic literature:

1. R. Mollin, *An introduction to Cryptography*, 2nd edition, Chapman and Hall/CRC Press, Boca Raton, 2007.
2. N. Koblitz, *A Course in number theory and cryptography*, Springer-Verlag, New York, 1994.
3. M. J. Hinek, *Cryptanalysis of* RSA *and its variants*, Chapman and Hall/CRC Press, Boca Raton, 2010.

Recommended literature:

1. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.
2. S. C. Coutinho, *The mathematics of ciphers; number theory and* RSA *criptography*, A. K. Peters, Natick, Massachusetts, 1999.
3. A. J. Menezes, P. C. Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.