Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Algebraiczne aspekty kryptografii**
Name in english	:	**Algebraic aspects of cryptography**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	optional
Course code	:	E2_W39
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	75	105			
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3	3			
including the number of points corresponding to the classes of practical (P)		3			
including the number of points corresponding occupations requiring direct contact (BK)	2	2			

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Presentation of basic algebraic tools used in public key cryptography.

C2 Strengthening the knowledge from the lecture, developing basic intuitions.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows the basic of the finite fields arithmetic.

W2 Understands the number fields sieve.

W3 Understands the Pohlig-Hellman algorithm.

W4 Knows basics of the arithmetic on the elliptic curves.

W5 Understans connections between the LLL algorithm and searching for GCD.

The student skills:

U1 The student is able to define requirements for choosing programming libraries in order to implement cryptographic algorithms.

U2 Is able to avoid basic mistakes in selecting public keys.

U3 Can implement arithmetic of elliptical curves.

The student's social competence:

K1 He/She is prepared to acquire new competences and cooperate with experts in other fields, especially in the field of efficiency and security of information systems.

K2 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Fundamental theorems utilized by the course.	3h
Wy2	Finite fields.	3h
Wy3	Factorization problem of RSA moduli n.	4h
Wy4	The Discrete Logarithm Problem and the basic methods of solving it.	5h
Wy5	Elliptic curves.	10h
Wy6	Lattices. The Lenstra-Lenstra-Lovasz algorithm.	5h
Type of classes - exercises		
Ćw1	Fundamental theorems utilized by the course.	3h
Ćw2	Finite fields.	3h
Ćw3	RSA moduli factorization.	4h
Ćw4	The Discrete Logarithm Problem.	6h
Ćw5	Elliptic curves.	10h
Ćw6	The LLL algorithm.	4h

Applied learning tools
1. Traditional lecture 2. Solving tasks and problems 3. Solving programming tasks 4. Consultation 5. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS		
Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W5, K1-K2	Final test.
F2	U1-U3, K1-K2	Evaluation of the implementation tasks.
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING
1. Neal Koblitz: A Course in Number Theory and Cryptography, Springer, Graduate Texts in Mathematics Series 2. Joachim von zur Gathen, Jurgen Gerhard: Modern Computer Algebra, 3rd Cambridge University Press New York, NY, USA 2013

SUPERVISOR OF COURSE
dr Przemysław Kubiak

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
Algebraic aspects of cryptography
WITH EFFECTS OF EDUCATION ON THE DIRECTION OF COMPUTER SCIENCE

Course training effect	Reference to the effect of the learning outcomes defined for the field of study and specialization (if applicable)	Objectives of the course**	The contents of the course**	Number of teaching tools**
W1	K2_W01 K2_W02	C1	Wy1-Wy6	1 4 5
W2	K2_W01 K2_W02	C1	Wy1-Wy6	1 4 5
W3	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
W4	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
W5	K2_W03 K2_W04	C1	Wy1-Wy6	1 4 5
U1	K2_U03 K2_U05	C2	Ćw1-Ćw6	2 3 4 5
U2	K2_U02 K2_U05	C2	Ćw1-Ćw6	2 3 4 5
U3	K2_U01 K2_U03	C2	Ćw1-Ćw6	2 3 4 5
K1	K2_K03 K2_K10	C1 C2	Wy1-Wy6 Ćw1-Ćw6	1 2 3 4 5
K2	K2_K03 K2_K10	C1 C2	Wy1-Wy6 Ćw1-Ćw6	1 2 3 4 5