Zał. nr 5 do ZW 16/2020

Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Algorytmiczna teoria liczb**
Name of the course in english	:	**Algorithmic Number Theory**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	W04INA-SM4010G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	15		15		
The total number of hours of student workload (CNPS)	25		35		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	1		1		
including the number of points corresponding to the classes of practical (P)			1		
including the number of points corresponding occupations requiring direct contact (BK)	1		1		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Presentation of basic algorithms and number theoretic dependencies used in public key cryptography.

C2 Practice of the knowledge gained during the lecture.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows modular arithmetic.

W2 Knows the rules used to determine the structure of an abelian group, knows the notion of the order of group element.

W3 Understands the presented algorithm for taking square roots in finite fields.

The student skills:

U1 Using SageMath the student is able to generate test vectors for his/her own implementations.

U2 Is able to optimize the discussed algorithms for some special input data.

U3 Is able to locate errors in an implementations of the discussed number theoretic algorithms.

The student's social competence:

K1 Understands a role of algebra in cryptography.

K2 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Congruences.	1h
Wy2	Groups, rings, fields, prime fields.	2h
Wy3	Inversion of an element: by the Fermat's Little Theorem and by the Extended Euclidean Algorithm.	2h
Wy4	Quadratic residues and quadratic nonresidues. Lagrange and Jacobi symbols.	2h
Wy5	Taking square roots in a prime field: the Tonelli-Shanks Algorithm and the algorithm by Siguna Mueller.	2h
Wy6	Structure of finite abelian groups. The multiplicative group of a prime field.	3h
Wy7	The order of group's element and the algorithm for finding it.	3h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	SageMath package.	3h
Lab2	Finding inversion of a nonzero element of a field.	4h
Lab3	Taking sqare roots in a prime field.	4h
Lab4	The order of group element.	4h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
3. Consultation
4. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS		
Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K2	Final test.
F2	U1-U3, K1-K2	Evaluation of the solutions of the lists of tasks.
P=0.4%*F1+0.6%*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

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Algorytmiczna teoria liczb

WITH LEARNING OUTCOMES IN THE FIELD OF ALGORITHMIC COMPUTER SCIENCE

Subject learning effect	Relating the subject effect to the learning outcomes defined for the field of study	Objectives of the course**	Program content**	Teaching tool number**
W1	K2_W01 K2_W02	C1	Wy1-Wy7	1 3 4
W2	K2_W01 K2_W02	C1	Wy1-Wy7	1 3 4
W3	K2_W03 K2_W04	C1	Wy1-Wy7	1 3 4
U1	K2_U01 K2_U03 K2_U05	C2	Lab1-Lab4	2 3 4
U2	K2_U02 K2_U05	C2	Lab1-Lab4	2 3 4
U3	K2_U01 K2_U03	C2	Lab1-Lab4	2 3 4
K1	K2_K03 K2_K10	C1 C2	Wy1-Wy7 Lab1-Lab4	1 2 3 4
K2	K2_K03 K2_K10	C1 C2	Wy1-Wy7 Lab1-Lab4	1 2 3 4