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	:	**Krzywe Eliptyczne dla Programistów**
Name of the course in english	:	**Elliptic Curves for Developers**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	W04INA-SM4113G
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	80		100		
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

Knowledge of the content of the course Ąlgorithmic Number Theory"is highly recommended.

COURSE OBJECTIVES

C1 Review of algorithms and data structures used in cryptography based on elliptic curves.

C2 Practice of the knowledge gained during the lecture.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Understands the reasons why elliptical curves have gained popularity in cryptography.

W2 He/She knows the different representations of the points of an elliptic curve.

W3 Understands the attacks on implementation errors or errors in parameter selection.

The student skills:

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

U2 Is able to locate errors in an implementations of the discussed algorithms.

U3 In SageMath he/she can verify the maps between different representations of a curve: Montgomery, Weierstrass, etc.

The student's social competence:

K1 Can carry out tasks pragmatically and creatively.

COURSE CONTENT		
Type of classes - lectures		
Wy1	Field characteristic and short Weierstrass form.	2h
Wy2	Addition and doubling formulas.	2h
Wy3	Point compression, Hasse theorem, what co-factor means.	2h
Wy4	ECDSA, ECDH.	1h
Wy5	Different coordinate systems: projective, jacobian.	6h
Wy6	Projective coordinates Leak.	4h
Wy7	Twisted curves. Why brainpool curves are better than NIST ones?	6h
Wy8	Montgomery Ladder - resistance to simple side-channel analysis.	1h
Wy9	Montgomery curves, twisted Edwards curves.	6h
	Sum of hours	30h
Type of classes - laboratory		
Lab1	The Discrete Logarithm Problem. Pollard-rho Method.	2h
Lab2	The Discrete Logarithm Problem on Elliptic Curves (EC). Pollard-rho Method on EC.	8h
Lab3	Jacobian coordinates leak.	6h
Lab4	Scalar multiplication algorithm that does not use y-coordinate.	4h
Lab5	Foult injection attack and moving the point on the twisted curve.	4h
Lab6	Mappings between Weierstrass, Montgomery and (twisted) Edwards form.	6h
	Sum of hours	30h

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-K1	Final test
F2	U1-U3, K1-K1	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
2. Andreas Enge: Elliptic Curves and Their Applications to Cryptography
3. Darrel Hankerson, Alfred J.Menezes, Scott Vanstone: Guide to Elliptic Curve Cryptography

SUPERVISOR OF COURSE

dr Przemysław Kubiak

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Krzywe Eliptyczne dla Programistów
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_W02 K2_W03 K2_W04	C1	Wy1-Wy9	1 3 4
W2	K2_W02 K2_W03	C1	Wy1-Wy9	1 3 4
W3	K2_W02 K2_W03	C1	Wy1-Wy9	1 3 4
U1	K2_U03 K2_U06	C2	Lab1-Lab6	2 3 4
U2	K2_U03 K2_U06	C2	Lab1-Lab6	2 3 4
U3		C2	Lab1-Lab6	2 3 4
K1	K2_K02 K2_K03	C1 C2	Wy1-Wy9 Lab1-Lab6	1 2 3 4