

Faculty of Fundamental Problems of Technology						
COURSE CARD						
Name in polish	:	Krzywe eliptyczne				
Name in english	:	Elliptic curves				
Field of study	:	Computer Science				
Specialty (if applicable)	:					
Undergraduate degree and form of	:	masters, stationary				
Type of course	:	optional				
Course code	:	E2_W34				
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)		90	90			
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)		3	3			
PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS						
COURSE OBJECTIVES						
<p>C1 Review of algebraic structures used in cryptography and selected protocols based on them.</p> <p>C2 Deepen the knowledge gained during the lecture.</p>						
COURSE LEARNING OUTCOMES						
<p>The scope of the student's knowledge:</p> <p>W1 Knows the notions: group, ring, field.</p> <p>W2 Know the constructions of elliptic, hyperelliptic curves, and notions of ideal class group</p> <p>W3 Knows some protocols based on elliptic and hyperelliptic curve and understands advantages of such solutions.</p> <p>The student skills:</p> <p>U1 Can check choosen properties discussed sructures.</p> <p>U2 Can implement discussed algorithms.</p> <p>The student's social competence:</p> <p>K1 Understands a role of algebra in informatics, especially in cryptography.</p>						
COURSE CONTENT						

Type of classes - lectures		
Wy1	Group Theory.	2h
Wy2	Rings and moduls.	4h
Wy3	Fields.	4h
Wy4	Projective space.	2h
Wy5	Projective geometry	2h
Wy6	Algebraic sets and groups.	2h
Wy7	Elliptic group	4h
Wy8	Elliptic Group over finite field.	2h
Wy9	Elliptic-curve cryptography	4h
Wy10	Hyperelliptic group.	2h
Wy11	Ideal class group.	2h

Type of classes - exercises		
Ćw1	Group Theory.	2h
Ćw2	Rings and Modules.	4h
Ćw3	Fields.	4h
Ćw4	Projective space.	2h
Ćw5	Projective Geometry.	2h
Ćw6	Algebraic groups.	2h
Ćw7	Elliptic Curve.	2h
Ćw8	Elliptic curve over finite Fields.	2h
Ćw9	Elliptic curve cryptosystems.	4h
Ćw10	Hyperelliptic Curve.	2h
Ćw11	Ideal class group.	2h

Applied learning tools
<ol style="list-style-type: none"> 1. Traditional lecture 2. Solving tasks and problems 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	
F2	U1-U2, K1-K1	
$P = \%*F1 + \%*F2$		

BASIC AND ADDITIONAL READING
<ol style="list-style-type: none"> 1. N. Koblitz, Algebraic Aspects of Cryptography. 2. S. Lang, Algebra.

SUPERVISOR OF COURSE
dr Krzysztof Majcher

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE

Elliptic curves

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_W02 K2_W03_B K2_W04_B	C1	Wy1-Wy11	1 3 4
W2	K2_W02 K2_W03_B	C1	Wy1-Wy11	1 3 4
W3	K2_W02 K2_W03_B	C1	Wy1-Wy11	1 3 4
U1	K2_U01_B K2_U09_B	C2	Ćw1-Ćw11	2 3 4
U2	K2_U01_B K2_U09_B K2_U12_B	C2	Ćw1-Ćw11	2 3 4
K1	K2_K01_B K2_K14_B	C1 C2	Wy1-Wy11 Ćw1-Ćw11	1 2 3 4