Zał nr 4 do ZW

Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Aspekty wydajności i bezpieczeństwa algorytmów kryptograficznych**
Name in english	:	**Efficiency and security aspects of cryptographic algorithms**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	optional
Course code	:	`E2_W40`
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	15	15		
The total number of hours of student workload (CNPS)	75	45	60		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	2	2	2		
including the number of points corresponding to the classes of practical (P)		2	2		
including the number of points corresponding occupations requiring direct contact (BK)	2	1	1		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Course: Algebraic aspects of cryptography.

COURSE OBJECTIVES

C1 Learning the basics of efficient implementation and side channel protection of protocols currently in place.

C2 Strengthening the knowledge from the lecture, developing intuition.

C3 Acquiring programming skills related to the subject of the lecture.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows the basic exponentiation algorithms implemented in cryptographic libraries.

W2 Knows advantages of Montgomery and Edwards curves.

W3 Knows basic randomization techniques.

W4 Understands the Miller's algorithm

The student skills:

U1 Is able to indicate the algorithm appropriate for a given problem.

U2 He is able to select the parameters of a given algorithm properly.

U3 Is able to broaden his/her knowledge of the lecture by analyzing available implementations and scientific papers.

The student's social competence:

K1 Is able to critically evaluate existing implementations of cryptographic algorithms in terms of efficiency and safety.

K2 It is prepared to acquire new competences and cooperate with experts from other fields, especially in the field of efficiency and security of designed IT systems.

K3 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Fast exponentiation techniques	8h
Wy2	Constant time exponentiation - Montgomery ladder, Lucas sequences	4h
Wy3	Fast elliptic curves - their arithmetic, and scalar multiplication	6h
Wy4	Side channel prevention: randomization techniques	4h
Wy5	Pairing computation	8h

Type of classes - exercises		
Ćw1	Fast exponentiation techniques	4h
Ćw2	Constant time exponentiation - Montgomery ladder, Lucas sequences	2h
Ćw3	Fast elliptic curves - their arithmetic, and scalar multiplication	3h
Ćw4	Side channel prevention: randomization techniques	2h
Ćw5	Pairing computation	4h

Type of classes - laboratory		
Lab1	Fast exponentiation techniques	5h
Lab2	Fast elliptic curves - their arithmetic, and scalar multiplication	6h
Lab3	Side channel prevention: randomization techniques	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-W4, K1-K3	Final test
F2	U1-U3, K1-K3	Short test
F3	U1-U3, K1-K3	Evaluation of programming tasks
P=40%*F1+20%*F2+40%*F3		

BASIC AND ADDITIONAL READING

1. Ben Lynn: On the implementation of pairing-based cryptosystems, dissertation, Stanford University (2007)
2. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters: Twisted Edwards Curves. AFRICACRYPT 2008: 389-405
3. Daniel J. Bernstein, Tanja Lange: Montgomery curves and the Montgomery ladder. IACR Cryptology ePrint Archive 2017: 293 (2017)
4. Donald Knuth: The Art of Computer Programming, Volume 2: Seminumerical Algorithms
5. Henri Cohen: A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics

SUPERVISOR OF COURSE

dr Przemysław Kubiak

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
Efficiency and security aspects of cryptographic algorithms
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 K2_W04	C1	Wy1-Wy5	1 4 5
W2	K2_W02 K2_W03 K2_W04	C1	Wy1-Wy5	1 4 5
W3	K2_W02 K2_W03 K2_W04	C1	Wy1-Wy5	1 4 5
W4	K2_W02 K2_W03 K2_W04	C1	Wy1-Wy5	1 4 5
U1	K2_U01 K2_U02	C2 C3	Ćw1-Ćw5 Lab1-Lab3	2 3 4 5
U2	K2_U01 K2_U02 K2_U04	C2 C3	Ćw1-Ćw5 Lab1-Lab3	2 3 4 5
U3	K2_U01 K2_U02 K2_U04	C2 C3	Ćw1-Ćw5 Lab1-Lab3	2 3 4 5
K1	K2_K01	C1 C2 C3	Wy1-Wy5 Ćw1-Ćw5 Lab1-Lab3	1 2 3 4 5
K2	K2_K03	C1 C2 C3	Wy1-Wy5 Ćw1-Ćw5 Lab1-Lab3	1 2 3 4 5
K3	K2_K07	C1 C2 C3	Wy1-Wy5 Ćw1-Ćw5 Lab1-Lab3	1 2 3 4 5