Zał. nr 6 do ZW 121/2020

Faculty of Information and Communication Technology

COURSE CARD

Name of the course in polish	:	**Kryptografia**
Name of the course in english	:	**Cryptography**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	I degree, stationary
Type of course	:	optional
Course code	:	E1_W35
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)	2	2			

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1

C2

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1

W2

The student skills:

U1

U2

The student's social competence:

K1

COURSE CONTENT

Type of classes - lectures		
Wy1	Cryptography overview	2h
Wy2	One time pad. Stream ciphers	4h
Wy3	Block ciphers, symmetric cryptography	4h
Wy4	Attacks on symmetric cryptography	2h
Wy5	Hash functions and their applications	2h
Wy6	RSA, asymmetric encryption, digital signatures	2h
Wy7	Asymmetric cryptography based on DLP	2h
Wy8	Public key infrastructure	2h
Wy9	Secure communication	2h
Wy10	Identification and authentication protocols	2h
Wy11	Zero Knowledge Proofs	2h
Wy12	Secret sharing, oblivious transfer	2h
Wy13	Crypto cryminality	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Solving cryptographic problems	30h
	Sum of hours	30h

Applied learning tools

1. Multimedia 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-W2, K1-K1	Final xam
F2	U1-U2, K1-K1	Assignements
P=60%*F1+40%*F2		

BASIC AND ADDITIONAL READING

1. Lecture Notes on Introduction to Cryptography, CMU, Vipul Goyal, available online
2. Cryptography. Theory and practice - Douglas R. Stinson
3. Lecture Notes on Cryptography - S. GoldwasserM. Bellare, available online
4. Handbook of Applied Cryptography, Paul C. van Oorschot , Scott A. Vanstone A. J. Menezes, available online

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski