Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Kryptografia**
Name in english	:	**Cryptography**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	compulsory
Course code	:	E2_I03
Group rate	:	Yes

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

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Standard knowledge of the field: abstract algebra, algorithms and data structures, probability, computational complexity.

COURSE OBJECTIVES

C1 presentation of advanced cryptographic techniques used in practice

C2 understanding advanced mechanisms of modern cryptography

C3 getting skills in implementing cryptographic techniques

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 knows most important techniques of modern cryptography

W2 knows tools and mathematical structures used to construct cryptographic schemes

W3 knows the most important problems and challenges of modern cryptography and cryptoanalysis

The student skills:

U1 is able to build cryptographic tools to ensure security

U2 is able to build and use cryptographic tools

U3 is able to use abstract mathematical structures used to implement cryptographic schemes

U4 is able to evaluate and select apropriate cryptographic schemes according to a set of given requirements

The student's social competence:

K1 understands need of use of cryptographic techniques

K2 is able to apply cryptographic techniques to the end-user needs and behaviours

K3 is able to adjust a cryptographic solution to the law and economical requirements

K4 is able to estimate and predict possible treads and attack surfaces

COURSE CONTENT

Type of classes - lectures		
Wy1	Cryptography - history and overview	2h
Wy2	One time pad. Stream ciphers	2h
Wy3	Block ciphers	2h
Wy4	PRPs and PRFs as block cipher abstractions	2h
Wy5	Message integrity. Collision resistant hash functions.	3h
Wy6	Security against active attacks - authenticate encryption	2h
Wy7	Discrete-log assumptions	2h
Wy8	Cryptography using arithmetic modulo composites	2h
Wy9	Security of cryptosystems based on factoring and discrete logarithm problem.	2h
Wy10	Digital signatures	2h
Wy11	Public-Key Cryptosystems in the Random Oracle Model	2h
Wy12	Zero knowledge proofs	2h
Wy13	Secure Multi Party Computation	2h
Wy14	Quantum cryptography	3h

Type of classes - exercises		
Ćw1	Ciphertext-only attacks	4h
Ćw2	Perfect secrecy	2h
Ćw3	Attacks on block ciphers	2h
Ćw4	Modes of operation	2h
Ćw5	Hash functions, message authentication codes	2h
Ćw6	CPA i CCA2	2h
Ćw7	Key agreement. ElGamal	2h
Ćw8	RSA	2h
Ćw9	Discrete logarithm, factoring	2h
Ćw10	Digital signatures	2h
Ćw11	Random Oracle Model	2h
Ćw12	Interactive proofs	2h
Ćw13	Oblivious transfer	2h
Ćw14	Quantum cryptography	2h

Type of classes - laboratory		
Lab1	How to implement a cryptographic provider	2h
Lab2	Securing data	2h
Lab3	Hash functions	2h
Lab4	Primality testing	2h
Lab5	Discrete logarithm	2h
Lab6	Factoring	2h
Lab7	Implementation of a chosen digital signature scheme	3h

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-W3, K1-K4	
F2	U1-U4, K1-K4	
F3	U1-U4, K1-K4	
P=%*F1+%*F2+%*F3		

BASIC AND ADDITIONAL READING

1. Introduction to modern cryptography. Jonathan Katz, Yehuda Lindell
2. Handbook of Applied Cryptography. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ISBN:0-8493-8523-7

SUPERVISOR OF COURSE
dr Filip Zagórski

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
Cryptography
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_W01 K2_W02 K2_W03 K2_W04	C1	Wy1-Wy14	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy14	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy14	1 4 5
U1	K2_U05 K2_U06 K2_U10 K2_U12	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U2	K2_U01 K2_U03 K2_U04 K2_U05 K2_U06 K2_U12 K2_U13	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U3	K2_U03 K2_U06	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
U4	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U11 K2_U12	C2 C3	Ćw1-Ćw14 Lab1-Lab7	2 3 4 5
K1	K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K2	K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K3	K2_K01 K2_K05	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K4	K2_K01 K2_K02 K2_K03 K2_K05 K2_K07 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5