Faculty of Information and Communication Technology/Department of Fundamentals of Computer Science

COURSE CARD

Name of the course in polish	:	**Bezpieczeństwo i prywatność w fazie projektowania**
Name of the course in english	:	**Security and Privacy by Design**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	W04INA-SM4007G
Group of courses	:	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)	30	30	30		
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	1	1	1		
including the number of points corresponding to the classes of practical (P)		1	1		
including the number of points corresponding occupations requiring direct contact (BK)	2	1	1		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Passed 'Security I' course.

COURSE OBJECTIVES

C1 Introduction to the formal analysis of security of information systems. Discussion of security models, types of attacks, adversaries and scenarios. Presentation of theorem proving techniques in the field of security.

C2 Provide the skills to: a) analyze the correctness of security protocols, b) prove security properties of selected systems for different models of adversaries.

C3 Design and prototype selected cryptosystems.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows mathematical models of access control and risk analysis

W2 Knows adversary models and attack scenarios

W3 Knows techniques for security proofs

The student skills:

U1 Specify security requirements for given systems in chosen models

U2 Analyse and evaluate security of given systems in chosen models

U3 Synthesize new systems from secure building blocks

The student's social competence:

K1 Describe and analyse computer security problems in chosen theoretical models.

K2 Understand and can argue for the need of theoretical analysis of computer security.

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to formal models of computer system security.	1h
Wy2	Adversary models and attack scenarios.	1h
Wy3	Formal models of cryptosystems and protocols security.	1h
Wy4	Proving security via reduction techniques.	1h
Wy5	Secure Identification.	5h
Wy6	Security digital Signatures.	5h
Wy7	Authenticated Key Establishment.	5h
Wy8	Secure schemes on untrusted devices.	5h
Wy9	Sequence of games with the adversary.	5h
Wy10	The framework of Universal Composability.	1h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Models.	1h
Ćw2	Proving security via reduction techniques.	8h
Ćw3	Proving security via sequence of games.	5h
Ćw4	Proving security in the UC Framework	1h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Implementing a prototype of a chosen security protocol.	15h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Solving tasks and problems
3. Creating programming projects
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-K2	
F2	U1-U3, K1-K2	
F3	U1-U3, K1-K2	
P=%*F1+%*F2+%*F3		

BASIC AND ADDITIONAL READING

1. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, Mihir Bellare and Phillip Rogaway
2. The Random Oracle Methodology Revisited, Ran Canetti, Oded Goldreich and Shai Halevi.
3. Abstract models of computation in cryptography, Ueli Maurer.
4. Universally Composable Security: A New Paradigm for Cryptographic Protocols, R. Canetti.

SUPERVISOR OF COURSE

dr hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Bezpieczeństwo i prywatność w fazie projektowania

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_W01 K2_W02 K2_W04	C1	Wy1-Wy10	1 4
W2	K2_W01 K2_W02 K2_W04	C1	Wy1-Wy10	1 4
W3	K2_W01 K2_W02 K2_W04	C1	Wy1-Wy10	1 4
U1	K2_U03 K2_U04 K2_U06	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U06 K2_U08	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
U3	K2_U02 K2_U03 K2_U04 K2_U06 K2_U08	C2 C3	Ćw1-Ćw4 Lab1-Lab1	2 3 4
K1	K2_K03 K2_K05 K2_K07	C1 C2 C3	Wy1-Wy10 Ćw1-Ćw4 Lab1-Lab1	1 2 3 4
K2	K2_K03 K2_K05 K2_K07	C1 C2 C3	Wy1-Wy10 Ćw1-Ćw4 Lab1-Lab1	1 2 3 4