Algorithmic Computer Science
second level - Cryptography and Computer Security
Course cards (2022)

Spis treści

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Bezpieczeństwo wysokopoziomowe - podatności i ataki**
Name of the course in english	:	**High level security - vulnerabilities and attacks**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4009G`
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)	60	45	45		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	2	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

Basic OS knowledge. Basic computer network knowledge. Programming knowledge.

COURSE OBJECTIVES

C1 Overview of hardware and software conditions related to the security of information systems. Discuss the vulnerabilities resulting from the limitations of the end-user platform, system design, and implementation. Presentation of attack scenarios, and detection methods.

C2 Case studies and synthetic examples. Scenarios exercises and pattern best practices.

C3 Master of software and system security testing in selected OS. Acquiring engineering skills in the field of detection / attack. Testing the effectiveness of attacks in a vulnerable virtual environment.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 knows security function and purpose of network devices and software

W2 knows application, data and host security threats and vulnerabilities

W3 knows concepts and practices related to authentication, authorization and access control

The student skills:

U1 can indicate vulnerabilities in IT security components.

U2 can exploit system vulnerabilities and attack faulty security components in IT systems.

U3 can attack badly designed crypto-systems.

The student's social competence:

K1 can describe and analyse chosen computer security problems in a comprehensive manner.

K2 understands needs of securing computer systems and can argue about it

K3 can use social engineering.

COURSE CONTENT

Type of classes - lectures		
Wy1	Definiowanie bezpiecznych funkcjonalności. Definiowanie ataku. Sposoby modelowania adwersarza.	5h
Wy2	Network Security.	8h
Wy3	Realisation errors.	10h
Wy4	Threats and Vulnerabilities.	7h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Synthetic attacks. Threats and Vulnerabilities.	1.0h
Ćw2	Attacks on identification scheme	1.5h
Ćw3	Attacks on privacy.	1.5h
Ćw4	Attacks on anonymity.	1.5h
Ćw5	Attacks on signature schemes.	1.5h
Ćw6	Fault variables and components binding.	1.5h
Ćw7	Fault randomisation usage.	1.0h
Ćw8	Attacks on secrecy.	1.5h
Ćw9	Errors in encryption schemes.	1.5h
Ćw10	Attacks on authenticated key establishment.	1.5h
Ćw11	Attacks based on randomness faults.	1.0h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Attacks in OSI Application Layer.	1h
Lab2	Bad design vulnerabilities. Social engineering attacks.	1h
Lab3	Web Application attacks. Hacking WebGoat.	1h
Lab4	SQL Injection attacks.	1h
Lab5	Broken Authentication.	2h
Lab6	XML external entities attacks	1h
Lab7	Cross Site Scripting (XSS).	1.5h
Lab8	Insecure deserialization.	1.5h
Lab9	Security misconfiguration.	2h
Lab10	Server-Side Request Forgery (SSRF).	1.5h
Lab11	Timing Attacks.	1.5h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Consultation
6. 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-K3	
F2	U1-U3, K1-K3	
F3	U1-U3, K1-K3	
P=%*F1+50%*F2+50%*F3		

BASIC AND ADDITIONAL READING

1. OWASP Mutillidae II Web Pen-Test Practice Application. https://sourceforge.net/projects/mutillidae/
2. CompTIA Security+ Study Guide: Exam SY0-101
3. Fundamentals of Computer Security
4. Penetration Testing with Kali Linux. https://www.kali.org/

SUPERVISOR OF COURSE

dr hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Bezpieczeństwo wysokopoziomowe - podatności i ataki
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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W10	C1	Wy1-Wy4	1 2 5 6
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12	C2 C3	Ćw1-Ćw11 Lab1-Lab11	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2 C3	Ćw1-Ćw11 Lab1-Lab11	3 4 5 6
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2 C3	Ćw1-Ćw11 Lab1-Lab11	3 4 5 6
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K10 K2_K12	C1 C2 C3	Wy1-Wy11 Ćw1-Ćw11 Lab1-Lab11	1 2 3 4 5 6
K2	K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K12	C1 C2 C3	Wy1-Wy4 Ćw1-Ćw11 Lab1-Lab11	1 2 3 4 5 6
K3	K2_K02 K2_K03 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K12	C1 C2 C3	Wy1-Wy4 Ćw1-Ćw11 Lab1-Lab11	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Procedury i Bezpieczeństwo Operacyjne**
Name of the course in english	:	**Compliance and Operational Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4001G`
Group of courses	:	Yes

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

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

Knows the basics of cryptology and computer security.

COURSE OBJECTIVES

C1 Presentation of the principles of a design and maintenance of an information security system in an enterprise or an institution.

C2 Teaching students the rules of creating documentation for an information security system.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows rules of risk analysis

W2 Knows legal, economical, and social aspects influencing security policies

W3 Knows vital normative and legal requirements for information security

W4 Knows concepts, architectures and roles of Security Information and Event Management (SIEM) and Security Operation Center (SOC)

W5 Knows basics principals of personal data protection stated by GDPR

W6 Knows concept of open banking and fundamental standards applies to the financial market - PSD2, RTS, PCI DSS

W7 Knows concept and rules of standardization of Common Criteria (CC)

The student skills:

U1 Is able to further develop her/his competences by reading standards, best practices and legal acts.

U2 Is able to correctly estimate impact and costs of security solutions proposed.

U3 Is able to see limitations of the methodology of information security management.

The student's social competence:

K1 Has competences in the design and implementation of security training.

K2 Can use project management techniques with respect to duties of security administrators.

K3 Able to perform tasks in a pragmatic and creative way.

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to cybersecurity issues, evet and incident definition, monitoring and logging	2h
Wy2	Security Information and Event Management (SIEM) and Security Operating Center (SOC)	2h
Wy3	Risk related concepts	2h
Wy4	Risk mitigation strategies	4h
Wy5	Incident response procedures	4h
Wy6	Security awareness	2h
Wy7	Business continuity	2h
Wy8	Environmental controls	2h
Wy9	Essentials of personal data protection defined by GDPR	2h
Wy10	Open baking and financial market standards - PSD2, RTS, PCI DSS	4h
Wy11	Disaster Recovery	3h
Wy12	The AIC (Availability, Integrity, Confidentiality) triad	1h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Analysis of selected Security Information and Event Management (SIEM) system	4h
Ćw2	Risk analysis.	4h
Ćw3	Analysis of selected case studies in terms of GDPR compliance	4h
Ćw4	Security policy, security plan and documented operating procedures.	6h
Ćw5	Incident response procedures.	6h
Ćw6	Contingency plan.	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
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-W7, K1-K3	evaluation of student’s answers given in the examination form
F2	U1-U3, K1-K3	evaluation of the documentation produced by the examined student
P=40%*F1+60%*F2		

BASIC AND ADDITIONAL READING

1. Krzysztof Liderman, Podręcznik administratora bezpieczeństwa teleinformatycznego, Wydawnictwo MIKOM, ISBN 8372793778
2. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations
3. NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems
4. NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems
5. ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements
6. ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management
7. ISO/IEC 27005 Information technology - Security techniques - Information security risk management
8. RFC 3227, Guidelines for Evidence Collection and Archiving

SUPERVISOR OF COURSE
dr inż. Wojciech Wodo

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Procedury i Bezpieczeństwo Operacyjne
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_W06 K2_W08	C1	Wy1-Wy12	1 2 4 5
W2	K2_W08 K2_W10	C1	Wy1-Wy12	1 2 4 5
W3	K2_W04 K2_W07 K2_W10	C1	Wy1-Wy12	1 2 4 5
W4	K2_W03 K2_W05 K2_W06 K2_W07 K2_W09	C1	Wy1-Wy12	1 2 4 5
W5	K2_W04 K2_W05 K2_W08	C1	Wy1-Wy12	1 2 4 5
W6	K2_W04 K2_W05 K2_W10	C1	Wy1-Wy12	1 2 4 5
W7	K2_W05 K2_W06 K2_W07	C1	Wy1-Wy12	1 2 4 5
U1	K2_U06 K2_U10 K2_U11	C2	Ćw1-Ćw6	3 4 5
U2	K2_U04 K2_U09 K2_U12	C2	Ćw1-Ćw6	3 4 5
U3	K2_U05 K2_U10	C2	Ćw1-Ćw6	3 4 5
K1	K2_K07	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5
K2	K2_K04 K2_K08 K2_K09	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5
K3	K2_K02 K2_K10	C1 C2	Wy1-Wy12 Ćw1-Ćw6	1 2 3 4 5

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Algorytmiczna teoria liczb**
Name of the course in english	:	**Algorithmic Number Theory**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4010G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	15		15		
The total number of hours of student workload (CNPS)	25		35		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	1		1		
including the number of points corresponding to the classes of practical (P)			1		
including the number of points corresponding occupations requiring direct contact (BK)	1		1		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Presentation of basic algorithms and number theoretic dependencies used in public key cryptography.

C2 Practice of the knowledge gained during the lecture.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows modular arithmetic.

W2 Knows the rules used to determine the structure of an abelian group, knows the notion of the order of group element.

W3 Understands the presented algorithm for taking square roots in finite fields.

The student skills:

U1 Using SageMath the student is able to generate test vectors for his/her own implementations.

U2 Is able to optimize the discussed algorithms for some special input data.

U3 Is able to locate errors in an implementations of the discussed number theoretic algorithms.

The student's social competence:

K1 Understands a role of algebra in cryptography.

K2 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Congruences.	1h
Wy2	Groups, rings, fields, prime fields.	2h
Wy3	Inversion of an element: by the Fermat's Little Theorem and by the Extended Euclidean Algorithm.	2h
Wy4	Quadratic residues and quadratic nonresidues. Lagrange and Jacobi symbols.	2h
Wy5	Taking square roots in a prime field: the Tonelli-Shanks Algorithm and the algorithm by Siguna Mueller.	2h
Wy6	Structure of finite abelian groups. The multiplicative group of a prime field.	3h
Wy7	The order of group's element and the algorithm for finding it.	3h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	SageMath package.	3h
Lab2	Finding inversion of a nonzero element of a field.	4h
Lab3	Taking sqare roots in a prime field.	4h
Lab4	The order of group element.	4h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
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-K2	Final test.
F2	U1-U3, K1-K2	Evaluation of the solutions of the lists of tasks.
P=0.4%*F1+0.6%*F2		

BASIC AND ADDITIONAL READING

1. Neal Koblitz: A Course in Number Theory and Cryptography, Springer, Graduate Texts in Mathematics Series
2. Joachim von zur Gathen, Jurgen Gerhard: Modern Computer Algebra, 3rd Cambridge University Press New York, NY, USA 2013

SUPERVISOR OF COURSE

dr Przemysław Kubiak

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Algorytmiczna teoria liczb
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	C1	Wy1-Wy7	1 3 4
W2	K2_W01 K2_W02	C1	Wy1-Wy7	1 3 4
W3	K2_W03 K2_W04	C1	Wy1-Wy7	1 3 4
U1	K2_U01 K2_U03 K2_U05	C2	Lab1-Lab4	2 3 4
U2	K2_U02 K2_U05	C2	Lab1-Lab4	2 3 4
U3	K2_U01 K2_U03	C2	Lab1-Lab4	2 3 4
K1	K2_K03 K2_K10	C1 C2	Wy1-Wy7 Lab1-Lab4	1 2 3 4
K2	K2_K03 K2_K10	C1 C2	Wy1-Wy7 Lab1-Lab4	1 2 3 4

Zał. nr 5 do ZW 16/2020

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

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	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4008G`
Group of courses	:	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.	2h
Wy6	Security against active attacks - authenticate encryption	2h
Wy7	Discrete-log assumptions	2h
Wy8	Cryptography using arithmetic modulo composites	2h
Wy9	Digital signatures	2h
Wy10	Secure Multi Party Computation. Obliovious transfer	2h
Wy11	Zero knowledge proofs	2h
Wy12	Bit commitments, verifiable secret sharing	2h
Wy13	Quantum cryptography	2h
Wy14	Post Quantum Cryptography	4h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Perfect secrecy. Ciphertext-only attacks	2h
Ćw2	Attacks on block ciphers	2h
Ćw3	Attacks on stream ciphers. Properties of pseudorandom generators	2h
Ćw4	Hash functions, message authentication codes. Properties of pseudorandom functions.	2h
Ćw5	Attacks on RSA. Integer factorization.	2h
Ćw6	Key agreement. ElGamal. Discreete log problem	2h
Ćw7	CPA and CCA	2h
Ćw8	Timing attacks on RSA implementation	2h
Ćw9	Oblivious transfer	2h
Ćw10	Interactive proofs. Zero-knowledge proofs	4h
Ćw11	Homomorphic encryption	2h
Ćw12	Secure multiparty computations	2h
Ćw13	Quantum cryptography	2h
Ćw14	Post-Quantum cryptography	2h
	Sum of hours	30h

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
	Sum of hours	15h

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 3. Cryptography. Theory and practice - Douglas R. Stinson 4. The Foundations of Cryptography (https://www.wisdom.weizmann.ac.il/ oded/foc-drafts.html) - Oded Goldreich 5. Lecture Notes on Cryptography (https://cseweb.ucsd.edu/ mihir/papers/gb.pdf) - S. Goldwasser, M. Bellare

SUPERVISOR OF COURSE
dr Filip Zagórski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Kryptografia

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_W03 K2_W04	C1	Wy1-Wy14	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08	C1	Wy1-Wy14	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08	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_K08 K2_K09 K2_K10	C1 C2 C3	Wy1-Wy14 Ćw1-Ćw14 Lab1-Lab7	1 2 3 4 5
K3	K2_K01 K2_K05 K2_K09 K2_K12	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

Zał. nr 5 do ZW 16/2020

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

Name of the course in polish	:	**Kwestie prawne w bezpieczeństwie komputerowym**
Name of the course in english	:	**Legal Issues in Computer Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4117G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30				
The total number of hours of student workload (CNPS)	90				
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3				
including the number of points corresponding to the classes of practical (P)					
including the number of points corresponding occupations requiring direct contact (BK)	2				

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

knowledge of the English language going beyond technical terminology

COURSE OBJECTIVES

C1 skills to interpret legal regulations and other requirements related to cybersecurity issues

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 knowledge of the technical implications of EU computer security regulations

W2 awareness of the processes of creating and implementing requirements

W3 knows the system of technical recommendations and certification

The student skills:

U1 can interpret legal requirements in terms of compatible technical products

U2 can adjust the IT system in terms of legal requirements and standards

U3 is able to assess the risks resulting from the implementation of requirements

The student's social competence:

K1 can cooperate with specialists in the field of law

K2 can cooperate with specialists in the field of formal certification systems

COURSE CONTENT

Type of classes - lectures		
Wy1	personal data protection	6h
Wy2	eIDAS regulation	4h
Wy3	ETSI, ICAO norms and role of standardization groups	4h
Wy4	e-Privacy concept	2h
Wy5	NIS regulation	2h
Wy6	European certification system	2h
Wy7	Common Criteria framework	6h
Wy8	chosen BSI recommendations	2h
Wy9	the system of RFC documents	2h
	Sum of hours	30h

Applied learning tools

1. Multimedia lecture
2. Solving tasks and problems
3. 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, U1-U3, K1-K2	tests, homeworks
P=100%*F1		

BASIC AND ADDITIONAL READING

1. current legal regulations concerning safety in the European Union, eur-lex.europa.eu service
2. FIPS norms
3. BSI recommendations
4. ENISA recommendations
5. European ETSI norms

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Kwestie prawne w bezpieczeństwie komputerowym
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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 3
W2	K2_W01 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 3
W3	K2_W01 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 3
U1	K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C1	Wy1-Wy9	2 3
U2	K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C1	Wy1-Wy9	2 3
U3	K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C1	Wy1-Wy9	2 3
K1	K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1	Wy1-Wy9	1 2 3
K2	K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1	Wy1-Wy9	1 2 3

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Systemy Wbudowane w Bezpieczeństwie Komputerowym**
Name of the course in english	:	**Embedded Security Systems**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4005G`
Group of courses	:	Yes

	Lectures	Exercises	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	60		90		
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	2		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

Fluency in programming, designing efficient algorithms, estimating computational complexity. Basic knowledge on computer systems architecture, operating systems and communication protocols and electronics.

COURSE OBJECTIVES

C1 presentation of architecture, limitations, functionalities and vulnerabilities of embedded systems in security area

C2 developing analysis skills of embedded systems, communication with them and conducting reverse engineering

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows design and architecture, programming and limits of embedded systems

W2 Knows communication standards used in embedded systems e.g. IrDA, UART, JTAG

W3 Knows basic principles and steps in embedded operating system analysis

W4 Knows specificity of embedded system vulnerabilities (side channel analysis, hardware-based trojans)

W5 Knows concept of SDR, programing GNU Radio and signal analysis

The student skills:

U1 Capability to conduct process of analysis of embedded system

U2 Capability to establish communication and conduct reverse engineering process of embedded system

U3 Capability to detect and exploit the vulnerabilities of embedded system

U4 Capability to design requirements for embedded system following security and privacy requirements

U5 Capability to program an Arduino microcontroller and communicate with peripherals

U6 Capability to utilize modules and protocols like IrDA, UART, SDR

The student's social competence:

K1 can design a system with respect to the expected social behaviour of its users

K2 can estimate the risk factor for a functioning system

K3 can create solutions oblivious to the end-user

K4 can estimate the potential of criminal activities

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to the embedded systems - reconnaissance	2h
Wy2	Hardware and software reverse engineering	6h
Wy3	Trusted Platform Module (TPM and Hardware Security Module (HSM)	2h
Wy4	Embedded systems vulnerabilities	2h
Wy5	Hardware-based trojans	2h
Wy6	Software Defined Radio (SDR)	2h
Wy7	GSM and SIM card	2h
Wy8	Automotive security	2h
Wy9	Physical Unclonable Functions (PUFs)	2h
Wy10	Side-channel attacks and analysis	4h
Wy11	Kleptography	2h
Wy12	Smart cards and modern ID documents	2h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	Assembling toolbox for working with embedded system	4h
Lab2	Establishing communication with embedded systems (e.g. UART)	4h
Lab3	Reverse engineering of selected embedded system	10h
Lab4	Remote analysis of embedded system vulnerabilities	6h
Lab5	Black-box embedded system analysis in a form of Arduino module	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Creating programming projects
5. Consultation
6. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W5, K1-K4	
F2	U1-U6, K1-K4	
P=%*F1+%*F2		

BASIC AND ADDITIONAL READING

1. Smart Card Handbook. Wolfgang Rankl, Wolfgang Effing, ISBN: 978-0-470-74367-6
2. Theoretical Aspects of Distributed Computing in Sensor Networks. Nikoletseas, Sotiris; Rolim, José, ISBN: 978-3-642-14848-4
3. Handbook of Sensor Networks. Yang Xiao, Hui Chen, Frank Haizhon Li, ISBN: 978-981-283-730-1
4. Embedded Systems Design with Platform FPGAs: Principles and Practices. Ronald Sass , Andrew G. Schmidt, ISBN:0123743338
5. Embedded Systems: A Contemporary Design Tool. James K. Peckol. ISBN: 0471721808
6. normative documents

SUPERVISOR OF COURSE

dr inż. Wojciech Wodo

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Systemy Wbudowane w Bezpieczeństwie Komputerowym
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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W4	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
W5	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 5 6
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12	C2	Lab1-Lab5	3 4 5 6
U4	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U5	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
U6	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab5	3 4 5 6
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K2	K2_K02 K2_K07 K2_K08 K2_K09 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K3	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6
K4	K2_K03 K2_K05 K2_K07 K2_K09 K2_K10 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab5	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Komunikacja i Infrastruktura Bezpieczeństwa**
Name of the course in english	:	**Communication and Security Infrastructure**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4011G`
Group of courses	:	Yes

	Lectures	Exercises	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	50		70		
Assesment	exam				
For a group of courses final course mark	X				
Number of ECTS credits	2		2		
including the number of points corresponding to the classes of practical (P)			2		
including the number of points corresponding occupations requiring direct contact (BK)	2		2		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Learning the fundamental protocols and data structures used for authentication and to secure communication.

C2 Learning the libraries implementing the protocols discussed during the lectures and learning tools for testing them.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 He/she knows the functionalities and purpose of the basic protocols used to secure communication.

W2 He knows the algorithms used by the above-mentioned protocols.

W3 He knows what are the most popular libraries implementing the above-mentioned protocols.

The student skills:

U1 Can implement specific functionalities of the above-mentioned protocols using mechanisms delivered by popular libraries.

U2 He can effectively test the implemented functionalities based on generally available tools and packages.

The student's social competence:

K1 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Public Key Infrastructure - X.509 Certificates, hierarchy, crosscertification (X-certification)	6h
Wy2	TLS protocol	6h
Wy3	IPSec	6h
Wy4	LDAP + SASL	6h
Wy5	DNSSec	4h
Wy6	Protocols and management of WIFI networks networks.	2h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	openssl	6h
Lab2	openswan/libreswan/strongswan	6h
Lab3	OpenLDAP, Apache Directory Studio, web2ldap, python-ldap	7h
Lab4	Cyrus SASL	7h
Lab5	OpenDNSSEC	4h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
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	Final test
F2	U1-U2, K1-K1	Evaluation of the solutions of the lists of tasks
P=0.4%*F1+0.6%*F2		

BASIC AND ADDITIONAL READING

1. RFC 5280, 5246, 8446, 6071, 4511, 4033-4035
2. https://www.openssl.org/
3. https://openswan.org/
4. https://www.opendnssec.org/

SUPERVISOR OF COURSE

dr Przemysław Kubiak

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Komunikacja i Infrastruktura Bezpieczeństwa
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_W03 K2_W04 K2_W07	C1	Wy1-Wy6	1 3 4
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W07	C1	Wy1-Wy6	1 3 4
W3	K2_W03 K2_W06 K2_W07	C1	Wy1-Wy6	1 3 4
U1	K2_U03 K2_U06 K2_U10 K2_U13	C2	Lab1-Lab5	2 3 4
U2	K2_U01 K2_U02 K2_U03 K2_U10 K2_U13	C2	Lab1-Lab5	2 3 4
K1	K2_K02 K2_K04 K2_K09 K2_K10	C1 C2	Wy1-Wy6 Lab1-Lab5	1 2 3 4

Zał. nr 5 do ZW 16/2020

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

Name of the course in polish	:	**Laboratorium Programowania w Cyberbezpieczeństwie**
Name of the course in english	:	**Software Engineering Lab in Cybersecurity**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4012G`
Group of courses	:	Yes

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

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 acquisition of practical programming skills on one of the key platforms for ensuring security

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 learn about one of the selected systems (FPGA, graphics cards, cryptographic cards, Android, ...)

W2 has knowledge in the field of building documentation of secure IT systems

W3 has knowledge in the field of product quality testing and evaluation

The student skills:

U1 ability to design a solution specification

U2 ability to create software in accordance with the regime of a specific system

U3 can test software among others regarding security aspects

U4 is able to present the final documentation covering security aspects for the audit

The student's social competence:

K1 the ability to design the product according to the real threats of social engineeringering

K2 is able to implement a project based on non-technical specifications resulting from business needs

K3 is able to implement projects in a transparent manner for audit certification

COURSE CONTENT

Type of classes - laboratory		
Lab1	basics of hardware/software architecture	6h
Lab2	principles of building secure software	2h
Lab3	designing solution specification	2h
Lab4	software implementation	10h
Lab5	product testing and optimization	8h
Lab6	final evaluation	2h
	Sum of hours	30h

Applied learning tools

1. Solving programming tasks
2. Creating programming projects
3. 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, U1-U4, K1-K3	implementation of programming tasks
P=100%*F1		

BASIC AND ADDITIONAL READING
1. technical documentation for the software/hardware used

SUPERVISOR OF COURSE
prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Laboratorium Programowania w Cyberbezpieczeństwie
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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Lab1-Lab6	3
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Lab1-Lab6	3
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Lab1-Lab6	3
U1	K2_U03 K2_U05 K2_U06 K2_U10 K2_U12 K2_U13	C1	Lab1-Lab6	1 2 3
U2	K2_U03 K2_U05 K2_U06 K2_U09 K2_U10 K2_U11 K2_U13	C1	Lab1-Lab6	1 2 3
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C1	Lab1-Lab6	1 2 3
U4	K2_U05 K2_U07 K2_U08 K2_U10 K2_U12 K2_U13	C1	Lab1-Lab6	1 2 3
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1	Lab1-Lab6	1 2 3
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1	Lab1-Lab6	1 2 3
K3	K2_K01 K2_K03 K2_K04 K2_K05 K2_K07 K2_K09 K2_K10 K2_K11 K2_K12	C1	Lab1-Lab6	1 2 3

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Fizyka i Obliczenia Kwantowe**
Name of the course in english	:	**Quantum Physics and Computing**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM4013G`
Group of courses	:	Yes

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

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

knowledge of basic tools of mathematical analysis

COURSE OBJECTIVES

C1 knowledge of the principles of quantum computing

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 basic knowledge of quantum physics sufficient to understand quantum algorithms

W2 has knowledge about the limitations and opportunities of quantum computing

W3 knows fundamental quantum algorithms and protocols

The student skills:

U1 can understand a quantum algorithm

U2 can estimate the computational complexity of a quantum algorithm

U3 can evaluate the usefulness of a quantum system

The student's social competence:

K1 Ability to evaluate the economics and applicability of quantum computing

K2 is aware of risks related to unconventional computational methods

COURSE CONTENT

Type of classes - lectures		
Wy1	physical foundations for quantum systems for quantum computing and communication	5h
Wy2	qubits and quantum gates	2h
Wy3	protocols of quantum communication	2h
Wy4	breaking Discrete Logarithm Problem	2h
Wy5	quantum algorithm for factorization	2h
Wy6	Grover's algorithm	2h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, U1-U3, K1-K2	tests
P=100%*F1		

BASIC AND ADDITIONAL READING

1. CERN Academic Training Lectures: Heather Gray, Introduction to Quantum Computing, available online
2. Quantum Computing: Lecture Notes, Ronald de Wolf (QuSoft, CWI and University of Amsterdam), arXiv:1907.09415

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Fizyka i Obliczenia Kwantowe

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_W03 K2_W04 K2_W05 K2_W07	C1	Wy1-Wy6	1 2
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy6	1 2
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W07	C1	Wy1-Wy6	1 2
U1	K2_U05 K2_U08 K2_U12 K2_U13	C1	Wy1-Wy6	
U2	K2_U03 K2_U04 K2_U05 K2_U06 K2_U08	C1	Wy1-Wy6	
U3	K2_U08 K2_U10 K2_U11 K2_U12 K2_U13	C1	Wy1-Wy6	
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K08 K2_K10 K2_K11	C1	Wy1-Wy6	1 2
K2	K2_K02 K2_K03 K2_K04 K2_K08 K2_K09 K2_K10 K2_K11	C1	Wy1-Wy6	1 2

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Praca Magisterska**
Name of the course in english	:	**MSc Thesis**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM0006D`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)					
The total number of hours of student workload (CNPS)	600				
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits					
including the number of points corresponding to the classes of practical (P)					
including the number of points corresponding occupations requiring direct contact (BK)					

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

COURSE OBJECTIVES

C1 Conducting independent research and writing a master's thesis

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Learn a new topic of Computer Science

W2 He will learn about the principles of writing scientific works

The student skills:

U1 Able to build an application related to the study problem

U2 Able to read the professional literature

U3 Can write a scientific paper

U4 He can prepare a professional multimedia presentation

The student's social competence:

K1 Demonstrates the intellectual independence

K2 Is able to work with other people

COURSE CONTENT

Module for writing a MSc thesis. It typically contains the analysis of literature, conducting preliminary research, the construction of the appropriate application, analyzys the properties of the application / conduct relevant research, thesis writing, preparing presentations, and preparation for the MSc exam.

Applied learning tools

1. Solving tasks and problems
2. Consultation
3. 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, U1-U4, K1-K2	The quality of the master's thesis
P=100%*F1		

BASIC AND ADDITIONAL READING

1. literature recommended by the promoter
2. documentation of tools used to implement applications

SUPERVISOR OF COURSE

prof. Jacek Cichoń

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Praca Magisterska

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_W04 K2_W05 K2_W06 K2_W09	C1		2 3
W2	K2_W05 K2_W10	C1		2 3
U1	K2_U01 K2_U02 K2_U03 K2_U04	C1	Wy1-Wy2	1 2 3
U2	K2_U06 K2_U08 K2_U11 K2_U13	C1	Wy1-Wy2	1 2 3
U3	K2_U06 K2_U07 K2_U08 K2_U10 K2_U11 K2_U12	C1	Wy1-Wy2	1 2 3
U4	K2_U08	C1	Wy1-Wy2	1 2 3
K1	K2_K01 K2_K02 K2_K03 K2_K10	C1		1 2 3
K2	K2_K01 K2_K02 K2_K04 K2_K05 K2_K10 K2_K12	C1		1 2 3

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Seminarium Magisterskie**
Name of the course in english	:	**MSc Seminar**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	compulsory
Course code	:	`W04INA-SM0003S`
Group of courses	:	Yes

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

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

The admission to the third semester of study

COURSE OBJECTIVES

C1 Discussion and clarification of the objectives of the thesis, to know the rules of editing theses, building presentations, and communicating the results (monitoring individual progress)

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows how to write scientific papers

The student skills:

U1 Knows Latex

U2 Can write presentations

U3 Can give a short lecture

The student's social competence:

K1 Understands the concept of plagiarism

K2 Able to briefly discuss a problem from IT

COURSE CONTENT

Type of classes - seminar		
Sem1	Discussion of rules of writing theses	2h
Sem2	Discussion about subjects of thesis	8h
Sem3	Analysis of thesis	10h
Sem4	Rules of writing prezentations	2h
Sem5	Participants prezentations	8h
	Sum of hours	30h

Applied learning tools

1. Solving tasks and problems
2. Creating multimedia presentations by students
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-W1, U1-U3, K1-K2	
P=%*F1		

BASIC AND ADDITIONAL READING

1. Literature consulted with thesis supervisor
2. Latex tutorial
3. Beamer tutorial

SUPERVISOR OF COURSE

prof. Jacek Cichoń

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Seminarium Magisterskie
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_W06 K2_W08 K2_W10	C1	Sem1-Sem5	3 4
U1	K2_U08	C1	Sem1-Sem5	1 2 3 4
U2	K2_U06 K2_U08	C1	Sem1-Sem5	1 2 3 4
U3	K2_U06 K2_U08 K2_U09	C1	Sem1-Sem5	1 2 3 4
K1	K2_K02 K2_K05 K2_K12	C1	Sem1-Sem5	1 2 3 4
K2	K2_K04 K2_K07 K2_K08 K2_K12	C1	Sem1-Sem5	1 2 3 4

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

COURSE CARD

Name of the course in polish	:	**Algorytmy rozproszone**
Name of the course in english	:	**Distributed Algorithms**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4101G`
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)	90	45	45		
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 OBJECTIVES

C1 Overview of basic techniques and algorithms used in a distributed environment

C2 Practicing skills in the construction of distributed algorithms

C3 Practical implementation of distributed algorithms as well as design and implementation of distributed algorithms in a selected environment

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 He knows the problems of designing distributed algorithms

W2 He knows the distributed algorithms presented in the lecture

W3 He knows the techniques of distributed algorithm analysis

The student skills:

U1 Can implement an application that uses distributed algorithms

U2 He can program algorithms distributed in different environments for distributed programming

U3 Is able to carry out a formal analysis of the correctness of a distributed algorithm

The student's social competence:

K1 Can explain the importance of distributed programming

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction	2h
Wy2	Model of communication and measures of complexity	4h
Wy3	Election algorithms	2h
Wy4	Logical time and clocks	2h
Wy5	Broadcasting and convergecast algorithms	2h
Wy6	Routing	2h
Wy7	The problem of consensus	2h
Wy8	The problem of diffuse mutual exclusion	2h
Wy9	Termination detection	4h
Wy10	Deadlock Detection	4h
Wy11	Damage detection	2h
Wy12	Self-stabilization	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Design and analysis of distributed algorithms	2h
Ćw2	Model of communication and measures of complexity	2h
Ćw3	Election algorithms	2h
Ćw4	Broadcasting and convergecast algorithms	2h
Ćw5	Routing and the problem of consensus	2h
Ćw6	The problem of distributed mutual exclusion	2h
Ćw7	Detection of termination, deadlock, damage	2h
Ćw8	Self-stabilization	1h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Getting to know the selected environment for the implementation of distributed systems	4h
Lab2	Implementation of distributed algorithms presented during the lecture and exercises	8h
Lab3	Techniques for processing big data (e.g. Map-Reduce)	3h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Consultation
6. 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	None
F2	U1-U3, K1-K1	Test
F3	U1-U3, K1-K1	Checking the fulfillment of task lists
P=0%*F1+50%*F2+50%*F3		

BASIC AND ADDITIONAL READING

1. Hagit Attiya, Jennifer Welch, Distributed Computing: Fundamentals, Simulations and Advanced Topics
2. Gerard Tel, Introduction to Distributed Algorithms
3. Ajay D. Kshemkalyani, Mukesh Singhal, Distributed Computing: Principles, Algorithms, and Systems

SUPERVISOR OF COURSE

dr inż. Marcin Zawada

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Algorytmy rozproszone
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_W03 K2_W04	C1	Wy1-Wy12	1 2 5 6
W2	K2_W02 K2_W04	C1	Wy1-Wy12	1 2 5 6
W3	K2_W01 K2_W02	C1	Wy1-Wy12	1 2 5 6
U1	K2_U01 K2_U02 K2_U05	C2 C3	Ćw1-Ćw8 Lab1-Lab3	3 4 5 6
U2	K2_U02 K2_U03	C2 C3	Ćw1-Ćw8 Lab1-Lab3	3 4 5 6
U3	K2_U03 K2_U04	C2 C3	Ćw1-Ćw8 Lab1-Lab3	3 4 5 6
K1	K2_K01 K2_K03 K2_K04 K2_K07	C1 C2 C3	Wy1-Wy12 Ćw1-Ćw8 Lab1-Lab3	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Data Mining**
Name of the course in english	:	**Data Mining**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4102G`
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)	70	55	55		
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

It is required to pass the following modules: Introduction to the Computer Science and Programming, Data Bases and Information Managements, Logic and Formal Structures, Probabilistic Methods and Statistic.

COURSE OBJECTIVES

C1 Presentation of the methods of data mining

C2 Profound understanding of the presented data mining methods

C3 Ability to use selected algorithms in practice

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows the data mining algorithms

W2 Knows the applicatinon of the data mining algorithms

The student skills:

U1 Can use the data mining algorithms in practice

U2 Can use the Apache Spark platform for efficient processing of large datasets

The student's social competence:

K1 Has the ability to cooperate with other experts specialized in data mining algorithms

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to the Data Mining	2h
Wy2	Building and evaluating the model	2h
Wy3	Linear regression and related methods	4h
Wy4	Resampling methods	2h
Wy5	Classification algororithms	6h
Wy6	Dimensionality reduction	4h
Wy7	Unsupervised learning	2h
Wy8	Effective implementation of machine learning algorithms	4h
Wy9	Analysis of data streams	4h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Model design and evaluation	2h
Ćw2	Linear regression	2h
Ćw3	Resampling methods	2h
Ćw4	Classification algororithms	5h
Ćw5	Dimensionality reduction	2h
Ćw6	Unsupervised learning	2h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Preparing Data for Mining	2h
Lab2	Linear regression and related methods	2h
Lab3	Classification algororithms	4h
Lab4	Clustering algororithms	2h
Lab5	Introduction Apache Spark	5h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. 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	Test
F2	U1-U2, K1-K1	Activity
F3	U1-U2, K1-K1	Implementation and presentation of solutions
P=40%*F1+30%*F2+30%*F3		

BASIC AND ADDITIONAL READING
1. The Elements of Statistical Learning: Data Mining, Inference, and Prediction, T.Hastie, R. Tibshirani, J.Friedman, 2009 2. Mining of Massive Datasets, J.Leskovec, A.Rajaraman, J. Ullman, 2010 3. Big Data Analytics with Spark, M. Guller, 2015

SUPERVISOR OF COURSE
dr inż. Jakub Lemiesz

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Data Mining
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 K2_W07	C1	Wy1-Wy9	1 2 6
W2	K2_W02 K2_W04	C1	Wy1-Wy9	1 2 6
U1	K2_U03 K2_U05 K2_U06 K2_U12	C2 C3	Ćw1-Ćw6 Lab1-Lab5	3 4 5 6
U2	K2_U01 K2_U03 K2_U05 K2_U06 K2_U13	C2 C3	Ćw1-Ćw6 Lab1-Lab5	3 4 5 6
K1	K2_K02 K2_K03 K2_K04 K2_K07 K2_K08 K2_K10	C1 C2 C3	Wy1-Wy9 Ćw1-Ćw6 Lab1-Lab5	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Zastosowania Metod Stochastycznych dla Bezpieczeństwa i Ochrony Prywatności**
Name of the course in english	:	**Applied Stochastics with Applications for Security and Privacy**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4103G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	60	120			
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

background in probability theory

COURSE OBJECTIVES

C1 presentation of techniques originating from probability theory and stochastic processes for applications in computer security technologies

C2 skills in using advanced techniques for computer security

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 posesses knowledge of discrete stochastic processes and their convergence

W2 understands threats and protection mechanisms agaist traffic analysis

W3 knows theoretical background of systems based on random processes

W4 knows self-stabilization and self-organization techniques

W5 understands the mechanisms of infection in distributed systems

W6 understands randomized algorithms used for generating and distribution of cryptographic data

The student skills:

U1 can analyze performance of a stochastic process

U2 can design and analyze solutions for defense against traffic analysis

U3 can apply random systems for construction of computer applications

U4 can design systems based on self-* paradigm

U5 can analyze processes in IT systems based on branching processes

The student's social competence:

K1 has skills for creating an abstract mathematical model for situations occuiring in practicein

COURSE CONTENT

Type of classes - lectures		
Wy1	Stochastic processes, Markov chains	4h
Wy2	Rapid mixing of Markov chains	4h
Wy3	Anonymous communication protocols, mix nets	4h
Wy4	Analysis of anonymity of Bitcoin transactions	4h
Wy5	Statistical tests	4h
Wy6	Security of pseudorandom generators and stream ciphers	4h
Wy7	Anomaly detection in systems	4h
Wy8	Risk-limiting audits	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Stochastic processes, Markov chains	4h
Ćw2	Rapid mixing of Markov chains	4h
Ćw3	Anonymous communication protocols, mix nets	2h
Ćw4	Random graphs and random walks	4h
Ćw5	Security systems based on random walk paradigm	2h
Ćw6	Self-stabilizing and self-organizing systems	2h
Ćw7	Branching processes, percolation and virus propagation	2h
Ćw8	Statistical tests. Anomaly detection	10h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. Creating multimedia presentations by students
7. Consultation
8. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W6, K1-K1	Project
F2	U1-U5, K1-K1	Home assignments
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. Introduction to Probability. C. M. Grinstead, J. L. Snell
2. Probability and Random Processes. G. R. Grimmett and D. R. Stirzaker, ISBN: 0198534485
3. Random Graphs. Svante Janson, Tomasz Luczak, Andrzej Rucinski. ISBN: 0471175412
4. Markov Chains and Mixing Times. David A. Levin, Yuval Peres and Elizabeth L. Wilmer, ISBN: 0821847392
5. Finite Markov Chains and Algorithmic Applications - O. Haggstrom
6. A Gentle Introduction to Risk-limiting Audits - Mark Lindeman and Philip B. Stark

SUPERVISOR OF COURSE

dr Filip Zagórski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Zastosowania Metod Stochastycznych dla Bezpieczeństwa i Ochrony Prywatności
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_W05	C1	Wy1-Wy8	1 2 7 8
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W3	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W4	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W5	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
W6	K2_W01 K2_W02 K2_W04 K2_W05	C1	Wy1-Wy8	1 2 7 8
U1	K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
U2	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U3	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U4	K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10	C2	Ćw1-Ćw8	3 4 5 6 7 8
U5	K2_U01 K2_U02 K2_U03 K2_U04 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
K1	K2_K02 K2_K03 K2_K05 K2_K06 K2_K07 K2_K10 K2_K12	C1 C2	Wy1-Wy8 Ćw1-Ćw8	1 2 3 4 5 6 7 8

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Wstęp do Elektroniki dla Systemów Bezpieczeństwa**
Name of the course in english	:	**Introduction to Electronics for Security Engineers**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4107G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	60	120			
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

Basic knowledge of electromagnetism and electricity derived from science classes at high-school level.

COURSE OBJECTIVES

C1 understanding fundamental mechanism of functionality of electronic systems

C2 skills in analysis and modelling of electronic systems

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 electronics background for information systems

W2 analytical models for fundamental electronic systems

W3 security technologies in electronics

The student skills:

U1 can adapt a computer system to security requirements taking into account electronics

U2 can analyze functionality of simple electronic components

U3 can design simple electronic components

U4 can carry out basic experiments and interpret the measurement results

The student's social competence:

K1 Can co-operate with electronic engineers - security specialists.

K2 Is capable of understanding non-polish literature on the subject.

K3 Can identify risks beyond his/her own field of expertise.

K4 Constructs requirements for software/hardware systems including information from other areas of knowledge.

COURSE CONTENT

Type of classes - lectures		
Wy1	Electronic properties of materials	2h
Wy2	Diodes and diode circuits	4h
Wy3	MOS transistors and biasing	2h
Wy4	MOS logic families	4h
Wy5	Bipolar transistors and logic families	4h
Wy6	Design parameters and issues	2h
Wy7	Storage elements	2h
Wy8	Interfacing logic families and standard buses	2h
Wy9	Amplifiers	2h
Wy10	Circuit modeling and simulation	2h
Wy11	Information leakage	2h
Wy12	Tamper evidence and resistance	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Current consumption in logic circuits.	4h
Ćw2	Random bits generation.	4h
Ćw3	Race condition in flip-flops. Random bits generation.	4h
Ćw4	Tapping of communcation bus.	4h
Ćw5	Radio sniffer.	4h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
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	test
F2	U1-U4, K1-K4	?
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. Charles Schuler: Electronics : principles & applications
2. Paul Horowitz, Winfield Hill: The art of electronics
3. SPICE: http://bwrc.eecs.berkeley.edu/classes/icbook/spice/

SUPERVISOR OF COURSE

dr inż. Przemysław Błaskiewicz

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Wstęp do Elektroniki dla Systemów Bezpieczeństwa

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_W03 K2_W04 K2_W05 K2_W09	C1	Wy1-Wy12	1 2 4 5
W2	K2_W01 K2_W02 K2_W04 K2_W07	C1	Wy1-Wy12	1 2 4 5
W3	K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy12	1 2 4 5
U1	K2_U03 K2_U05 K2_U06 K2_U11 K2_U12 K2_U13	C2	Ćw1-Ćw5	3 4 5
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw5	3 4 5
U3	K2_U01 K2_U02 K2_U03 K2_U06 K2_U08 K2_U12	C2	Ćw1-Ćw5	3 4 5
U4	K2_U04 K2_U05 K2_U08 K2_U12	C2	Ćw1-Ćw5	3 4 5
K1	K2_K02 K2_K03 K2_K06 K2_K07 K2_K09 K2_K10	C1 C2	Wy1-Wy12 Ćw1-Ćw5	1 2 3 4 5
K2	K2_K03 K2_K06 K2_K07 K2_K09	C1 C2	Wy1-Wy12 Ćw1-Ćw5	1 2 3 4 5
K3	K2_K02 K2_K03 K2_K07 K2_K09	C1 C2	Wy1-Wy12 Ćw1-Ćw5	1 2 3 4 5
K4	K2_K02 K2_K03 K2_K04 K2_K08 K2_K09 K2_K10	C1 C2	Wy1-Wy12 Ćw1-Ćw5	1 2 3 4 5

Zał. nr 5 do ZW 16/2020

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

Name of the course in polish	:	**Systemy Identyfikacyjne i Biometryczne**
Name of the course in english	:	**Identification and Biometric Systems**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4109G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	60	120			
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

Knowledge of information systems design principles. Basic skills in probability calculus and statistics.

COURSE OBJECTIVES

C1 Learning about biometric methods, construction of biometric-based identification systems, and demonstration of identification techniques using modern identity documents

C2 Getting skills and knowledge in designing identification systems based on biometrics and modern identity documents

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows technical details related to electronic identity cards

W2 Knows technical details related to biometric identification

W3 Understands mechanisms of errors in biometric identification procedures

W4 Knows how to protect personal data

W5 Knows the modern techniques of monitoring and anomaly detection by sensor systems

The student skills:

U1 Is able to design and implement an application using electronic ID cards

U2 Is able to design and implement an application using biometric readers

U3 Is able to analyse the risk of personal data leakage

U4 Is able to design a system storing and proceeding confidential data

U5 Is able to conduct analysis for the particular biometric identification system scenario, propose appropriate solution and tweak system parameters

The student's social competence:

K1 Is able to design/modify a solution to make it well suited to the economical/cultural environment

K2 Follows the rules of personal and biometric data protection

K3 Is able to train users of identification systems

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to biometric, fundamental properties and application	4h
Wy2	Errors of biometric systems (FAR and FRR, ROC and DET curve, CMC)	2h
Wy3	Testing, selection and comparison of biometric systems	2h
Wy4	Overview of biometric systems	8h
Wy5	Protection of biometric data	2h
Wy6	Physical monitoring based on identification systems	2h
Wy7	Reliability issues for biometric systems	2h
Wy8	Security of sensors and biometric system	2h
Wy9	Electronic identification documents	4h
Wy10	Legal and ethical aspects of biometrics	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Protocol analysis of protocols for electronic identification documents	4h
Ćw2	Design of applications based on electronic identity documents	2h
Ćw3	Analysis of biometrics	4h
Ćw4	Design of solutions based on biometric methods	4h
Ćw5	Management of sensitive information	4h
Ćw6	Analysis of solutions implementing cancelable biometrics	4h
Ćw7	Analysis of solutions for liveness testing and presentation attacks detection	4h
Ćw8	Analysis of solutions based on biometric fusion	4h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. Creating multimedia presentations by students
7. Consultation
8. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W5, K1-K3	final test
F2	U1-U5, K1-K3	short tests, tasks assignments
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents
2. Bindings:Guide to Biometrics. Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, ISBN: 1441923055
3. Anil Jain, Patrick Flynn, Arun A. Ross, “Handbook of Biometrics”, Springer-Verlag US, 2008

SUPERVISOR OF COURSE

dr inż. Wojciech Wodo

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Systemy Identyfikacyjne i Biometryczne
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 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy10	1 2 7 8
W2	K2_W01 K2_W02 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy10	1 2 7 8
W3	K2_W01 K2_W02 K2_W04 K2_W05 K2_W06 K2_W08 K2_W09	C1	Wy1-Wy10	1 2 7 8
W4	K2_W01 K2_W02 K2_W04 K2_W05 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy10	1 2 7 8
W5	K2_W01 K2_W02 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy10	1 2 7 8
U1	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U08 K2_U09 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
U2	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U08 K2_U09 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U08 K2_U10 K2_U12	C2	Ćw1-Ćw8	3 4 5 6 7 8
U4	K2_U03 K2_U05 K2_U06 K2_U09 K2_U10 K2_U12 K2_U13	C2	Ćw1-Ćw8	3 4 5 6 7 8
U5	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Ćw1-Ćw8	3 4 5 6 7 8
K1	K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K11 K2_K12	C1 C2	Wy1-Wy10 Ćw1-Ćw8	1 2 3 4 5 6 7 8
K2	K2_K05 K2_K07 K2_K08 K2_K09 K2_K11 K2_K12	C1 C2	Wy1-Wy10 Ćw1-Ćw8	1 2 3 4 5 6 7 8
K3	K2_K03 K2_K05 K2_K06 K2_K07 K2_K09 K2_K11 K2_K12	C1 C2	Wy1-Wy10 Ćw1-Ćw8	1 2 3 4 5 6 7 8

Zał. nr 5 do ZW 16/2020

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

Name of the course in polish	:	**Wykład Monograficzny**
Name of the course in english	:	**Monographic Lecture**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM0110G`
Group of courses	:	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

Prerequisites will be defined before the course starts

COURSE OBJECTIVES

C1 Presentation of new trends in IT

C2 Practical mastery of the tools and concepts discussed at the lecture

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Learn about new ideas Computer Science

The student skills:

U1 Can apply new solutions from Computer Science

The student's social competence:

K1 He understands the need to track new developments in Computer Science

COURSE CONTENT

Type of classes - lectures		
Wy1	Presentation of selected IT issues	30h
	Sum of hours	30h

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

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, K1-K1	Final test
F2	U1-U1, K1-K1	Activity on the exercises and practical implementation of the algorithms discussed in the lecture
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING
1. Literature will be given at the beginning of classes

SUPERVISOR OF COURSE
prof. Jacek Cichoń

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Wykład Monograficzny
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_W04 K2_W05	C1	Wy1-Wy1	1 4 5
U1	K2_U01 K2_U05 K2_U06 K2_U07 K2_U11 K2_U12	C2	Ćw1-Ćw1	2 3 4 5
K1	K2_K03	C1 C2	Wy1-Wy1 Ćw1-Ćw1	1 2 3 4 5

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Bezpieczne przetwarzanie w chmurze**
Name of the course in english	:	**Secure Cloud Computing**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4112G`
Group of courses	:	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

Knows and administers chosen OS.

COURSE OBJECTIVES

C1 The course targets: the security solutions for major platforms of cloud computing. The main goal is to review secure architectures, infrastructures, and software components using the user-centric and data-centric approach

C2 The goal is to: train security procedures in cloud computing platforms, gain practical attack/defend skills in remote and virtual environment.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows security aspects of hardware architectures for cloud computing

W2 Knows security aspects of software architectures for cloud computing.

W3 Knows cryptographic schema which of security extensions for cloud computing

The student skills:

U1 Can manage cloud software as a security administrator

U2 Can use client software and various extensions to provide secure data processing at cloud.

U3 Can configure remote user environment for secure computing.

The student's social competence:

K1 Can present arguments for securing remote computation.

K2 Can present legal aspects of cloud computing.

COURSE CONTENT

Type of classes - lectures		
Wy1	Data management	4h
Wy2	Durability of data in cloud.	6h
Wy3	Operation on common data.	6h
Wy4	Secure remote functionality.	4h
Wy5	Private information retrieval.	6h
Wy6	Secure multiparty computation	4h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	Identity and anonymous credentials management	10h
Lab2	Securing communication	10h
Lab3	Data management	8h
Lab4	Multiparty signatures	2h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks

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	List of Lab Exercises.
P=%*F1+100%*F2		

BASIC AND ADDITIONAL READING
1. Chosen OS documentation. 2. Chosen cloud platform documentation.

SUPERVISOR OF COURSE
dr hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Bezpieczne przetwarzanie w chmurze

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_W02 K2_W05 K2_W07	C1	Wy1-Wy6	1 2
W2	K2_W05 K2_W07	C1	Wy1-Wy6	1 2
W3	K2_W02 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy6	1 2
U1	K2_U05 K2_U06	C2	Lab1-Lab4	3 4
U2	K2_U03	C2	Lab1-Lab4	3 4
U3	K2_U05 K2_U06	C2	Lab1-Lab4	3 4
K1	K2_K01 K2_K09	C1 C2	Wy1-Wy6 Lab1-Lab4	1 2 3 4
K2	K2_K03 K2_K05	C1 C2	Wy1-Wy6 Lab1-Lab4	1 2 3 4

Zał. nr 5 do ZW 16/2020

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

Name of the course in polish	:	**Krzywe Eliptyczne dla Programistów**
Name of the course in english	:	**Elliptic Curves for Developers**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4113G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	80		100		
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

Knowledge of the content of the course Ą̧lgorithmic Number Theory"is highly recommended.

COURSE OBJECTIVES

C1 Review of algorithms and data structures used in cryptography based on elliptic curves.

C2 Practice of the knowledge gained during the lecture.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Understands the reasons why elliptical curves have gained popularity in cryptography.

W2 He/She knows the different representations of the points of an elliptic curve.

W3 Understands the attacks on implementation errors or errors in parameter selection.

The student skills:

U1 Using SageMath the student is able to generate test vectors for his/her own implementations.

U2 Is able to locate errors in an implementations of the discussed algorithms.

U3 In SageMath he/she can verify the maps between different representations of a curve: Montgomery, Weierstrass, etc.

The student's social competence:

K1 Can carry out tasks pragmatically and creatively.

COURSE CONTENT

Type of classes - lectures		
Wy1	Field characteristic and short Weierstrass form.	2h
Wy2	Addition and doubling formulas.	2h
Wy3	Point compression, Hasse theorem, what co-factor means.	2h
Wy4	ECDSA, ECDH.	1h
Wy5	Different coordinate systems: projective, jacobian.	6h
Wy6	Projective coordinates Leak.	4h
Wy7	Twisted curves. Why brainpool curves are better than NIST ones?	6h
Wy8	Montgomery Ladder - resistance to simple side-channel analysis.	1h
Wy9	Montgomery curves, twisted Edwards curves.	6h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	The Discrete Logarithm Problem. Pollard-rho Method.	2h
Lab2	The Discrete Logarithm Problem on Elliptic Curves (EC). Pollard-rho Method on EC.	8h
Lab3	Jacobian coordinates leak.	6h
Lab4	Scalar multiplication algorithm that does not use y-coordinate.	4h
Lab5	Foult injection attack and moving the point on the twisted curve.	4h
Lab6	Mappings between Weierstrass, Montgomery and (twisted) Edwards form.	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
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	Final test
F2	U1-U3, K1-K1	Evaluation of the solutions of the lists of tasks
P=0.4%*F1+0.6%*F2		

BASIC AND ADDITIONAL READING

1. Neal Koblitz: A Course in Number Theory and Cryptography
2. Andreas Enge: Elliptic Curves and Their Applications to Cryptography
3. Darrel Hankerson, Alfred J.Menezes, Scott Vanstone: Guide to Elliptic Curve Cryptography

SUPERVISOR OF COURSE

dr Przemysław Kubiak

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Krzywe Eliptyczne dla Programistów
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_W02 K2_W03 K2_W04	C1	Wy1-Wy9	1 3 4
W2	K2_W02 K2_W03	C1	Wy1-Wy9	1 3 4
W3	K2_W02 K2_W03	C1	Wy1-Wy9	1 3 4
U1	K2_U03 K2_U06	C2	Lab1-Lab6	2 3 4
U2	K2_U03 K2_U06	C2	Lab1-Lab6	2 3 4
U3		C2	Lab1-Lab6	2 3 4
K1	K2_K02 K2_K03	C1 C2	Wy1-Wy9 Lab1-Lab6	1 2 3 4

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Wykład Monograficzny z Bezpieczeństwa Komputerowego**
Name of the course in english	:	**Monographic Lecture on Computer Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4114G`
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)	60	60	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 OBJECTIVES

C1 Presentation of new trends in computer security

C2 Practical mastery of the tools and concepts discussed at the lecture

C3 mplementation and testing of problems presented during the lecture

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Learning new ideas in computer security

The student skills:

U1 Can apply new IT solutions

The student's social competence:

K1 Understands the need to track new achievements in IT

COURSE CONTENT

Type of classes - lectures		
Wy1	Presentation of selected computer security issues	30h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Solving problems discussed during the lecture	15h
	Sum of hours	15h

Type of classes - laboratory		
Lab1	Implementation and testing of problems discussed during the lecture	15h
	Sum of hours	15h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Consultation
6. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1, K1-K1	Final test
F2	U1-U1, K1-K1	Test, activity on exercises
F3	U1-U1, K1-K1	Issued implementations of problems
P=40%*F1+30%*F2+30%*F3		

BASIC AND ADDITIONAL READING

1. The literature will be given at the beginning of the class by the lecturer

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Wykład Monograficzny z Bezpieczeństwa Komputerowego
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_W04 K2_W05	C1	Wy1-Wy1	1 2 5 6
U1	K2_U01 K2_U05 K2_U06 K2_U11 K2_U12	C2 C3	Ćw1-Ćw1 Lab1-Lab1	3 4 5 6
K1	K2_K03	C1 C2 C3	Wy1-Wy1 Ćw1-Ćw1 Lab1-Lab1	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Cyfrowe Przetwarzanie Sygnałów**
Name of the course in english	:	**Digital Signal Processing**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4105G`
Group of courses	:	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

Knowledge of data structures and algorithms. Programming ability in a chosen programming language. Recommended courses: Introduction to Electronics, Scientific Calculations.

COURSE OBJECTIVES

C1 Presentation of the signal processing techniques used in computing and telecommunications.

C2 Mastering practical skills in selected DSP algorithms.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Student knows basics of signal physics. Student knows methods for signal conversion.

W2 Student knows transform and filter algorithms.

W3 Student knows techniques for image and audio analysis and processing.

The student skills:

U1 Student applies a proper mathematical techniques to compute various DSP algorithms.

U2 Student uses a variety of CAS and numerical computing environment in DSP.

U3 Student implements DSP algorithms in a chosen computer language.

The student's social competence:

K1 Student describes signals acquisition and processing for underlying physical processes.

K2 Student arguments the need for developing effective DSP methods.

COURSE CONTENT

Type of classes - lectures		
Wy1	Signal and process. Noise.	2h
Wy2	ADC and DAC conversion. Quantization.	3h
Wy3	Linear Systems.	3h
Wy4	Convolution.	3h
Wy5	Fourier analysis. Discrete Fourier transform.	3h
Wy6	Digital filters.	4h
Wy7	Audio processing.	3h
Wy8	Image processing.	3h
Wy9	Neural Networks	2h
Wy10	Digital Signal Processors	2h
Wy11	The Laplace Transform.	2h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	Convolution	5h
Ćw2	Fourier analysis. Discrete Fourier transform.	5h
Ćw3	Digital filters.	5h
Ćw4	Image and audio processing techniques.	5h
Ćw5	Neural Networks.	5h
Ćw6	The Laplace Transform.	5h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating multimedia presentations by students
6. 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	written test(s)
F2	U1-U3, K1-K2	points from student assignments
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. The Scientist and Engineer's Guide to Digital Signal Processing. Steven W. Smith, Ph.D. http://www.dspguide.com

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Cyfrowe Przetwarzanie Sygnałów
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_W03	C1	Wy1-Wy11	1 2 6
W2	K2_W02 K2_W03 K2_W04	C1	Wy1-Wy11	1 2 6
W3	K2_W01 K2_W03 K2_W04 K2_W05	C1	Wy1-Wy11	1 2 6
U1	K2_U02 K2_U03 K2_U04 K2_U06 K2_U08	C2	Ćw1-Ćw6	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U06	C2	Ćw1-Ćw6	3 4 5 6
U3	K2_U02 K2_U03 K2_U04 K2_U06	C2	Ćw1-Ćw6	3 4 5 6
K1	K2_K03 K2_K07 K2_K10	C1 C2	Wy1-Wy11 Ćw1-Ćw6	1 2 3 4 5 6
K2	K2_K02 K2_K07 K2_K10	C1 C2	Wy1-Wy11 Ćw1-Ćw6	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Blockchain i kryptowaluty**
Name of the course in english	:	**Blockchain and cryptocurrencies**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4118G`
Group of courses	:	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 Gaining knowledge on the technical mechanisms of cryptocurrencies, blockchain, smart contracts; learning skill for designing and implementation of secure systems based on these technologies

C2 ability to programme and analyse smart-contracts

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 understanding cryptographic and distributed systems background of blockchain, cryptocurrencies and smart contracts

W2 awareness of the level of security and reliability of the mechanisms being the subject of the lecture

W3 knowledge of the basics of smart contracts and methods of their implementation

The student skills:

U1 ability to implement a smart contract

U2 ability to evalate threats and security guarantees of systems based on the technologies in question

U3 the ability to use blockchain technology to build secure data repositories

The student's social competence:

K1 can determine pragmatic applications of the discussed technologies in the context of financial trading

K2 is able to correctly assess the sociological and psychological context of solutions

COURSE CONTENT

Type of classes - lectures		
Wy1	Introduction to cryptocurrencies	4h
Wy2	Consensus. Models, attacks. Nakamoto Consensus	4h
Wy3	Proof of work	2h
Wy4	Proof of space	2h
Wy5	Verifiable delay functions	2h
Wy6	Proof of stake	2h
Wy7	Privacy and mixing	2h
Wy8	zk-SNARKs	4h
Wy9	Smart-contract security	4h
Wy10	Ethereum	2h
Wy11	zCash	2h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	Managing wallets	2h
Lab2	Hands on with Ethereum	2h
Lab3	Smart contracts	2h
Lab4	ERC20 tokens and ICOs	2h
Lab5	Merkle trees	2h
Lab6	Ethereum attacks	2h
Lab7	zk-SNARKs	4h
Lab8	Mix-servers	4h
Lab9	Solidity	10h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Multimedia lecture
3. Solving tasks and problems
4. Solving programming tasks
5. Creating programming projects
6. 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	Exam
F2	U1-U3, K1-K2	Problem sets and final project
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING

1. Bitcoin's Academic Pedigree - Arvind Narayanan, Jeremy Clark
2. Bitcoin: A Peer-to-Peer Electronic Cash System - Satoshi Nakamoto
3. Foundations of Distributed Consensus and Blockchains - Elaine Shi
4. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER - DR. GAVIN WOOD
5. Solidity - https://docs.soliditylang.org/en/latest/
6. Zerocash: Decentralized Anonymous Payments from Bitcoin - Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza

SUPERVISOR OF COURSE

dr Filip Zagórski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Blockchain i kryptowaluty
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_W03 K2_W04 K2_W05 K2_W07 K2_W09	C1	Wy1-Wy11	1 2 6
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08 K2_W09	C1	Wy1-Wy11	1 2 6
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W08 K2_W09	C1	Wy1-Wy11	1 2 6
U1	K2_U01 K2_U05 K2_U06 K2_U10 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
U3	K2_U03 K2_U05 K2_U06 K2_U07 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab9	3 4 5 6
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy11 Lab1-Lab9	1 2 3 4 5 6
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy11 Lab1-Lab9	1 2 3 4 5 6

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Uczenie maszynowe i bezpieczeństwo**
Name of the course in english	:	**Machine Learning and Security**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4121G`
Group of courses	:	Yes

	Lectures	Exercises	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 Presentation of the application of machine learning (ML) to anomaly and threat detection in information systems. Overview of ML based network attacks detection. Presentation of the basic threats related to the ML process. Discussion of techniques ensuring the integrity of the inputs and outputs of the ML process. Overview of mechanisms ensuring the privacy and confidentiality of machine learning implemented on remote platforms. Discussion of the problem of provable remote training in ML processes.

C2 Implementation of selected anomaly detection techniques based on machine learning (ML). Practicing the implementation of selected methods that ensure privacy and confidentiality of ML processes.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 ML usage in anomaly and threats detection

W2 Awareness of threats and vulnerabilities related to ML processes

W3 Protection of ML processes

The student skills:

U1 can detect ML related anomalies and threats

U2 can identify threats and vulnerabilities related to ML processes

U3 can design and manage protection of ML processes

The student's social competence:

K1 can determine the security of solutions based on machine learning in the economic and social context

K2 can identify potential pragmatic application areas for machine learning

COURSE CONTENT

Type of classes - lectures		
Wy1	introduction to ML	4h
Wy2	ML based anomaly and threats detection	4h
Wy3	ML in Cloud	4h
Wy4	data Secrecy in ML	3h
Wy5	privacy in ML	3h
Wy6	training data injection, poisoning and mislabeling	3h
Wy7	secure Federated ML	3h
Wy8	secure ML using Homomorphic Encryption	3h
Wy9	proof of learning, proof of training	3h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	introduction to ML	6h
Lab2	ML based anomaly and threats detection	6h
Lab3	training data injection, poisoning and mislabeling	6h
Lab4	privacy and secrecy in ML	6h
Lab5	proof of learning, proof of training	6h
	Sum of hours	30h

Applied learning tools

1. Traditional lecture
2. Solving programming tasks
3. Creating programming projects
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-K2	
F2	U1-U3, K1-K2	Average of partial grades for solved lists of laboratory tasks.
P=%*F1+1%*F2		

BASIC AND ADDITIONAL READING

1. The literature will be given at the beginning of the class by the lecturer

SUPERVISOR OF COURSE

dr hab. inż. Łukasz Krzywiecki

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT

Uczenie maszynowe i bezpieczeństwo

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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy9	1 4 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 4 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W09 K2_W10	C1	Wy1-Wy9	1 4 5
U1	K2_U01 K2_U02 K2_U04 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab5	2 3 4 5
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Lab1-Lab5	1 2 3 4 5

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Złośliwe Mechanizmy i Techniki Ochrony**
Name of the course in english	:	**Malicious Mechanisms and Defence Techniques**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4119G`
Group of courses	:	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

knowledge of issues from the lecture on cryptography and algebraic number theory

COURSE OBJECTIVES

C1 acquiring knowledge and skills in the field of hostile software/hardware and methods of protection against it

C2 practical skills in implementing security countermeasures

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 understands the mechanisms used in the basic areas of operation of hostile IT products

W2 knows the mechanisms of preventing threats in the most important areas of attacks

W3 knows the mechanisms of protection against black box solutions

The student skills:

U1 is able to locate potential vulnerabilities and their determinants

U2 is able to design and implement protection using standard technical means

U3 is able to design and implement innovative protection mechanisms

The student's social competence:

K1 understands the mechanisms of social engineering and the attacks resulting from it

K2 is able to implement IT projects in a user-friendly and transparent manner

COURSE CONTENT

Type of classes - lectures		
Wy1	computer viruses and worms	2h
Wy2	attacks on password systems	2h
Wy3	security issues in P2P systems	4h
Wy4	web security	2h
Wy5	algorithms of distributed attacks	2h
Wy6	spam filtering	2h
Wy7	security problems of mobile devices	2h
Wy8	security mechanisms for IoT devices	4h
Wy9	subversion resilience mechanisms	2h
Wy10	watchdog mechanism	2h
Wy11	PUF	2h
Wy12	high level cryptographic protection	4h
	Sum of hours	30h

Type of classes - laboratory		
Lab1	tools for detecting and analyzing viruses, worms	2h
Lab2	attacking password systems	2h
Lab3	chosen P2P systems and studying their vulnerabilities	2h
Lab4	Web site vulnerabilities and security tools	4h
Lab5	defence against DDoS attacks	2h
Lab6	configuration of spam filtering	2h
Lab7	security mechanisms of Android	2h
Lab8	security design of smart meters	2h
Lab9	cryptographic protocols for protection against clones and loss of control over the device	4h
Lab10	protocols eliminating hidden channels	4h
Lab11	application of PUF mechanisms	2h
Lab12	emerging topics	2h
	Sum of hours	30h

Applied learning tools

1. Multimedia lecture
2. Solving tasks and problems
3. Solving programming tasks
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	tests
F2	U1-U3, K1-K2	
P=50%*F1+%*F2		

BASIC AND ADDITIONAL READING

1. Lecture Notes on “Computer and Network Security”, Avi Kak, Perdue Univ.

SUPERVISOR OF COURSE

prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Złośliwe Mechanizmy i Techniki Ochrony
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_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy12	1 4
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W08 K2_W09	C1	Wy1-Wy12	1 4
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W06 K2_W07 K2_W09 K2_W10	C1	Wy1-Wy12	1 4
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
U2	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U07 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
U3	K2_U01 K2_U02 K2_U03 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Lab1-Lab12	2 3 4
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K11 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab12	1 2 3 4
K2	K2_K01 K2_K03 K2_K04 K2_K05 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab12	1 2 3 4

Zał. nr 5 do ZW 16/2020

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

COURSE CARD

Name of the course in polish	:	**Technologie zwiększające prywatność**
Name of the course in english	:	**Privacy Enhancing Technologies**
Field of study	:	Algoritmic Computer Science
Specialty (if applicable)	:	
Level and form of studies	:	II degree, stationary
Type of course	:	optional
Course code	:	`W04INA-SM4120G`
Group of courses	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30	30			
The total number of hours of student workload (CNPS)	60	120			
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

knowledge of GDPR rules, knowledge and skills in cryptography

COURSE OBJECTIVES

C1 acquiring knowledge and skills in the field of privacy protection technologies

C2 gaining practical skills in the design and implementation of privacy protection

COURSE LEARNING OUTCOMES

The scope of the student’s knowledge:

W1 knows the mechanisms and limitations of anonymous communication

W2 knows the mechanisms of pseudonymization and anonymization

W3 knows the fundamental systems implementing privacy protection

The student skills:

U1 can evaluate the effectiveness of privacy protection mechanisms

U2 is able to design / choose a solution adequate to the needs

U3 has experience related to possibilities of breaking privacy protection

The student’s social competence:

K1 understanding and skills to consider requirements for privacy protection

K2 can estimate the risk and the level of reliability of privacy protection systems

COURSE CONTENT

Type of classes - lectures		
Wy1	anonymity measures and database protection	4h
Wy2	simulatability, deniability and other basic cryptographic mechanisms	2h
Wy3	pseudonimization techniques	2h
Wy4	pseudonymous signatures	4h
Wy5	authentication and key exchange protocols supporting privacy protection	4h
Wy6	protocols of anonymous communication	4h
Wy7	anonymous transactions and cryptocurrencies	4h
Wy8	malicious cryptography and methods for breaking privacy protection	2h
Wy9	e-voting	4h
	Sum of hours	30h

Type of classes - exercises		
Ćw1	activities sceanario due to GDPR	4h
Ćw2	differential privacy, database protection	2h
Ćw3	privacy protection in case of standard protocols	6h
Ćw4	pseudonimization and anonymization techniques	2h
Ćw5	privacy protection in ICAO standards	4h
Ćw6	TOR	2h
Ćw7	Monero protocols	2h
Ćw8	implementation of hostile cryptography for privacy breaches	4h
Ćw9	pragmatic e-voting systems	4h
	Sum of hours	30h

Applied learning tools
1. Multimedia lecture 2. Solving tasks and problems 3. Solving programming tasks 4. Creating programming projects 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-K2	tests
F2	U1-U3, K1-K2	problem solving, programming assignments
P=50%*F1+50%*F2		

BASIC AND ADDITIONAL READING
1. The literature will be given at the beginning of the class by the lecturer

SUPERVISOR OF COURSE
prof. Mirosław Kutyłowski

MATRIX OF LEARNING OUTCOMES FOR THE SUBJECT
Technologie zwiększające prywatność
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_W03 K2_W04 K2_W05 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 5
W2	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 5
W3	K2_W01 K2_W02 K2_W03 K2_W04 K2_W05 K2_W07 K2_W08 K2_W09 K2_W10	C1	Wy1-Wy9	1 5
U1	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U08 K2_U09 K2_U10 K2_U11 K2_U12 K2_U13	C2	Ćw1-Ćw9	2 3 4 5
U2	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Ćw1-Ćw9	2 3 4 5
U3	K2_U01 K2_U02 K2_U03 K2_U04 K2_U05 K2_U06 K2_U07 K2_U10 K2_U11 K2_U12 K2_U13	C2	Ćw1-Ćw9	2 3 4 5
K1	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Ćw1-Ćw9	1 2 3 4 5
K2	K2_K01 K2_K02 K2_K03 K2_K04 K2_K05 K2_K06 K2_K07 K2_K08 K2_K09 K2_K10 K2_K11 K2_K12	C1 C2	Wy1-Wy9 Ćw1-Ćw9	1 2 3 4 5