(*faculty stamp*) **COURSE DESCRIPTION**

1. Course title: COMPUTER SYSTEMS SECURITY	**2. Course code: CSS**
3. Validity of course description: 2017/2018	
4. Level of studies: 2nd cycle of higher education	
5. Mode of studies: intramural studies	
6. Field of study: MACROFACULTY	(RAU)
7. Profile of studies: general academic	
8. Programme: Informatics	
9. Semester: 2	
10. Faculty teaching the course: Faculty Of Automatic Control, Electronics and Informatics	
11. Course instructor: dr inż. Jacek Lach	
12. Course classification: -	
13. Course status: compulsory	
14. Language of instruction: English	

15. Pre-requisite qualifications:

It is assumed that the student has the basic knowledge of computer programming, operating systems and computer networks.

16. Course objectives:

Information being processed in computer systems became invaluable. To protect this information we have to use qualified tools and algorithms. Most of the mechanisms that are widely used today are secure. Most problems with security today stems from improper usage of strong security. The aim of the course is not only to present common security solutions but also to demonstrate some background knowledge which would help using proper tools for selected tasks and allow for building secure solutions.

17. Description of learning outcomes:

Nr	Learning outcomes description	Method of assessment	Teaching methods	Learning outcomes reference code
1.	Knowledge of basic techniques and methods of data security	SP, CL	WM, L	K2A_W15, K2A_W16
2.	Ability to use technical documentation of cryptographic algorithms	SP, CL	WM, L	K2A_U01
3.	Ability to properly use available implementations of cryptographic algorithms	SP, CL	WM, L	K2A_U06, K2A_K06
4.	Knowledge about basic cryptographic algorithms	SP, CL	WM, L	K2A_W15
5.	Knowledge about standard tools during estimation of security of networks and operating systems	SP, CL	WM, L	K2A_U01

18. Teaching modes and hours

Lecture / BA /MA Seminar / Class / Project / Laboratory

Lecture - 15 h, Class - , Laboratory – 15 h

19. Syllabus description:

Lectures includes the following topics:

Introduction to computer security. History, terms, basic components, threats, trust. Overview of security areas: computer networks, operating systems, transactional systems, telecommunication, e-voting, e-documents. Implementing security: cryptography I. Definition of cryptography. Classial cryposystems: transposition and substitution. Symmetric cryptosystems. Public key cryptosystems. Key management: key generation, key exchange,

key storage, key revocation. Key infrastructures: X.509, PGP.
Implementing security: cryptography II. Stream and block ciphers. Algorithms: DES, AES, RSA. Block cipher modes of operation. Randomness in computer system, how random is random(). Pseudo Random Number Generators. Stream ciphers. Hash functions. Digital signatures. Weakening strong ciphers – common problems. Strenghtening weak solutions – common solutions.
Security of data: storage systems. Encrypted filesystems, encrypted directories, encrypted containers. Whole-Disk encryption. Problems with disk encryption. Secure deletion of data.
Operating system security: access control, Bell-LaPadula model, security policies, capabilities, access control lists.
Authentication: something you know, something you have, something you are: passwords, tokens and biometrics. One time passwords. Dictionary attacks. System security evaluation – Common Criteria.
Network security: secure comunication, secure services. Security at different levels: application layer – mail security, spam, transport layer: SSL, network layer: IPSec.
Modern aspects of security: biocryptography, steganography, digital watermarking, visual cryptography.

The laboratories covers the following topics:

1. Penetration testing
2. Understanding cryptography – symmetric cryptography
3. Steganography

20. Examination: no

21. Primary sources:

- M. Bishop: Computer security. Art and science. Addison-Wesley. 2003
- J. Pieprzyk, T. Hardjono, J. Seberry: Fundamentals of Computer Security, Springer-Verlag, 2003
- A. J. Menezes, P. C. Van Oorschot, S.A. Vanstone: Handbook of applied cryptography, CRC Press, 1997

22. Secondary sources:

23. Total workload required to achieve learning outcomes

Lp.	Teaching mode :	Contact hours / Student workload hours
1	Lecture	15 / 15
2	Classes	- / -
3	Laboratory	15 / 15
4	Project	- / -
5	BA/ MA Seminar	- / -
6	Other	- / -
	Total number of hours	30 / 30

24. Total hours: 60

25. Number of ECTS credits: 2

26. Number of ECTS credits allocated for contact hours: 1

27. Number of ECTS credits allocated for in-practice hours (laboratory classes, projects): 2

26. Comments:

Approved:

…….
(date, Instructor's signature)

……
(*date , the Director of the Faculty Unit signature)*