Załącznik Nr 5 do Zarz. Nr 33/11/12

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

1. Course title: MATHEMATICS OF BLOCKCHAIN	**2. Course code: WM1**
3. Validity of course description: 2019/2020	
4. Level of studies: 2nd cycle of higher education	
5. Mode of studies: intramural studies	
6. Field of study: MATHEMATICS	(FACULTY SYMBOL) RMS
7. Profile of studies: general	
8. Programme: all	
9. Semester: III	
10. Faculty teaching the course: Faculty of Applied Mathematics	
11. Course instructor: professor Bogdana Oliynyk	
12. Course classification: course of limited choice	
13. Course status: monographic	
14. Language of instruction: English	
15. Pre-requisite qualifications: Mathematical Analysis, Algebra, Number Theory, English.	
16. Course objectives: The aim of the course is to familiarize students with number theoretic and algebraic foundations of cryptography, deal with main cryptographic algorithms and protocols, describe their usage in real world Blockchain applications.	

17. Description of learning outcomes:

A student who completes the course successfully should

Nr	Learning outcomes description	Method of assessment	Teaching methods	Learning outcomes reference code
1.	know examples of classic ciphers, understand concepts of one-pad encryption	test	lecture class	K2A_W01 K2A_W05 K2A_W11
2.	understand concepts of public-key cryptography, digital signatures, decentralized computations	test	lecture class	K2A_W11 K2A_W14 K2A_U18 K2A_K01 K2A_K06
3.	know basic concepts and properties of finite fields	test	lecture class	K2A_W11 K2A_U12 K2A_W02 K2A_K02
4.	know examples of public-key cryptography systems: RSA, Padded RSA, ECDLP, ECDSA	test	lecture class	K2A_W11 K2A_U12 K2A_K02 K2A_U18
5.	understand notion of cryptographic hash functions, know examples of cryptographic hash functions	test	lecture class	K2A_W05 K2A_W11 K2A_U18 K2A_K06
6.	understand concepts and constructions of cryptocurrencies	test	lecture class	K2A_W11 K2A_U12 K2A_K01 K2A_K06

18. Teaching modes and hours

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

Lecture 30h. Class 30h.

19. Syllabus description:

Lecture: Classic ciphers: basic concepts and examples. One-pad encryption. Public-key cryptography: main concepts, types of attacks, security. Design, main algorithms correctness and security main properties of RSA and Padded RSA. Discrete logarithm problem. The notion of a cryptographic hash functions, definitions and properties, method of construction, examples. Diffie-Hellman key exchange. 10. Digital signatures. Elliptic curves, elliptic-curve cryptography. Decentralized computations. Byzantine Fault Tolerance. Cryptocurrencies.

Class: Solve exercise approach to theory and examples presented at lecture

20. Examination: no

21. Primary sources:

1. Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, CHAPMAN & HALL/CRC, 2008.
2. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, Springer, 2008.
3. Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2018.
4. https://en.bitcoin.it/wiki/Main_Page

22. Secondary sources:

1. Neal Koblitz. Algebraic Aspects of Cryptography, Springer, 1999.
2. Christian Cachin, Marko Vukolić, Blockchain Consensus Protocols in the Wild, https://arxiv.org/abs/1707.01873.
3. www.iacr.org. International Association for Cryptologic Research (IACR).
4. https://www.nist.gov/publications/digital-signature-standard-dss-0 The National Institute of Standards and Technology (NIST) Digital Signature Standard (DSS).
5. L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, 1982.

23. Total workload required to achieve learning outcomes

Lp.	Teaching mode :	Contact hours / Student workload hours
1	Lecture	30/30
2	Classes	30/30
3	Laboratory	/
4	Project	/
5	BA/ MA Seminar	/
6	Other: consultations, use of e-learning webpage	/
	Total number of hours	60/60

24. Total hours: 120

25. Number of ECTS credits: 4

26. Number of ECTS credits allocated for contact hours: 4

27. Number of ECTS credits allocated for in-practice hours (laboratory classes, projects): 0

26. Comments:

Test I – 25 points, Test II – 25 points, Test III – 25 points, Test IV – 25 points,

To pass, it is necessary to obtain a total of 45 points, including at least 35% of the points of each learning outcome component.

Approved:

…….
(date, Instructor's signature)

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