COURSE DESCRIPTION CARD

Bialystok University of Technology Faculty of Electrical Engineering									
Field of study	**Erasmus**							**Degree level and programme type**	**Bachelor's degree Full time**
Specialisation/ diploma path	**-**							**Study profile**	**-**
Course name	**Cryptography**							**Course code**	**IS-FEE-10083S**
								Course type	**elective**
Forms and number of hours of educational activities	**L**	**C**	**LC**	**P**	**SW**	**FW**	**S**	**Semester**	**summer**
	30				**30**			**No. of ECTS credits**	**6**
Entry requirements	**-**								
Course objectives	Obtaining knowledge of different cryptography algorithms and techniques as well as their applications in securing of information systems. Acquisition of practical skills in performing computational analysis of different cryptography algorithms and its operations in selected technical security measures.								
Course content	<u>Lecture</u>: Introduction to cryptography and its applications. A brief historical overview of cryptography. Basic concepts of cryptography: encryption, decryption, symmetric key cryptography, and public key cryptography. Formal conditions of providing information confidentiality and integrity. Concept of Feistel Block Cipher. Constructions of contemporary symmetric ciphers: DES, AES. Modes of using block ciphers. The problem of multiple encryption. Constructions of contemporary asymmetric ciphers: RSA, ECC. Key distribution methods. Public key Intrastructure (PKI). Hybrid cryptography systems. Digital signatures and hash functions. Applications of cryptography for user and device authentication. Cryptography in web communication: SSL, TLS. <u>Specialization workshop</u>: Analysis of operation and effectiveness of selected cryptographic algorithms. Testing attacks on hash functions, also in the context of the effectiveness of password security in the case of disclosure of the user base of the ICT system. Configuration and testing of selected applications of cryptographic algorithms in the protection of information systems.								
Teaching methods	**Lecture, Specialization workshop**								
Assessment method	Lecture - written exam Specialization workshop - evaluation of reports, verification of preparation for classes, assessment of activity, written and oral tests								

Symbol of learning outcome	Learning outcomes	Reference to the learning outcomes for the field of study
	Knowledge: the graduate knows and understands	
LO1	main concepts and mathematical foundations of cryptographic algorithms,	
LO2	selected applications of cryptographic methods to ensure the security of information systems.	
	Skills: the graduate is able to	
LO3	perform a basic analysis of the operation and effectiveness of classical and modern cryptographic techniques,	
LO4	configure and test the operation of selected information protection systems based on cryptographic algorithms.	
	Social competence: the graduate is ready to	
LO5		
LO6		

Symbol of learning outcome	Methods of assessing the learning outcomes	Type of tuition during which the outcome is assessed
LO1	written exam	L
LO2	written exam	L
LO3	evaluation of reports, assessment of activity, short written quiz, final oral test.	SW
LO4	evaluation of reports, assessment of activity, short written quiz, final oral test.	SW
LO5		
LO6		

Student workload (in hours)		No. of hours
Calculation	lecture attendance	30
	revising of the content of subsequent lectures	15
	participation in student-teacher sessions (2L+3SW)	5
	preparation for the final exam	30
	participation in specialization workshop	30
	preparation for specialization workshop and work on reports	40
	TOTAL:	150

Quantitative indicators	HOURS	No. of ECTS credits
Student workload – activities that require direct teacher participation	65	2,6
Student workload – practical activities	73	2,9
Basic references	1. Stallings W.: Cryptography and Network Security: Principles and Practice, 8th edition, Pearson 2022. 2. W. Bray Shannon: Implementing Cryptography Using Python, Wiley 2020.	

Supplementary references	1. Stalling W., Brown L.: Computer Security: Principles and Practice, 4th edition, Pearson 2017. 2. Ortega J.M.: Mastering Python for Networking and Security, 2nd edition, Packt Publishing 2021.	
Organisational unit conducting the course	Department of Photonics, Electronics and Lighting Technology	Date of issuing the programme
Author of the programme	Andrzej Zankiewicz, PhD Eng.	03.02.2023

L – lecture, C – classes, LC – laboratory classes, P – project, SW – specialization workshop, FW - field work, S – seminar