



Subject card

Subject name and code	Foundations of Cryptography, PG_00048249						
Field of study	Informatics						
Date of commencement of studies	February 2023		Academic year of realisation of subject		2022/2023		
Education level	second-cycle studies		Subject group		Optional subject group Subject group related to scientific research in the field of study		
Mode of study	Full-time studies		Mode of delivery		at the university		
Year of study	1		Language of instruction		Polish		
Semester of study	1		ECTS credits		2.0		
Learning profile	general academic profile		Assessment form		exam		
Conducting unit	Department of Algorithms and Systems Modelling -> Faculty of Electronics, Telecommunications and Informatics						
Name and surname of lecturer (lecturers)	Subject supervisor		mgr inż. Andrzej Jastrzębski				
	Teachers		mgr inż. Andrzej Jastrzębski				
Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	15.0	0.0	0.0	0.0	30
	E-learning hours included: 0.0						
Learning activity and number of study hours	Learning activity	Participation in didactic classes included in study plan		Participation in consultation hours		Self-study	SUM
	Number of study hours	30		4.0		16.0	50
Subject objectives	Students learn basics of cryptography.						

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[K7_W01] Knows and understands, to an increased extent, mathematics to the extent necessary to formulate and solve complex issues related to the field of study.	Student learns mathematical foundations of cryptography.	[SW1] Assessment of factual knowledge
	[K7_U09] can carry out a critical analysis of the functioning of existing technical solutions and assess these solutions, as well as apply experience related to the maintenance of advanced technical systems, devices and facilities typical for the field of studies, gained in the professional engineering environment	Student learns how cryptosystems work.	[SU1] Assessment of task fulfilment
	[K7_W43] Knows and understands, to an increased extent, the nformal, technical and social aspects of the operation of complex information systems in the information society and in the global information n infrastructure.	Student learns advanced cryptosystems.	[SW1] Assessment of factual knowledge
	[K7_K02] is ready to provide critical evaluation of received content and to acknowledge the importance of knowledge in solving cognitive and practical problems	Student learns how to evaluate cryptosystems.	[SK5] Assessment of ability to solve problems that arise in practice
	[K7_U04] can apply knowledge of programming methods and techniques as well as select and apply appropriate programming methods and tools in computer software development or programming devices or controllers using microprocessors or programmable elements or systems specific to the field of study, making assessment and critical analysis of the prepared software as well as a synthesis and creative interpretation of information presented with it	Student implements basic cryptosystems.	[SU1] Assessment of task fulfilment
Subject contents	Introduction to modern cryptography. Classical cryptography: transposition and substitution ciphers, permutations. Modular arithmetic and RSA. Finite fields and AES. Symmetric and asymmetric cryptography.		
Prerequisites and co-requisites			
Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
		0.0%	100.0%
Recommended reading	Basic literature	D.R. Stinson: "Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications) 3rd Edition".	
	Supplementary literature	None.	
	eResources addresses	Adresy na platformie eNauczanie: Podstawy kryptografii 2023 - Moodle ID: 29726 https://enauczenie.pg.edu.pl/moodle/course/view.php?id=29726	
Example issues/ example questions/ tasks being completed			
Work placement	Not applicable		