



Subject card

Subject name and code	Cryptography, PG_00060224						
Field of study	Kryptografia						
Date of commencement of studies	October 2023		Academic year of realisation of subject			2025/2026	
Education level	first-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	3		Language of instruction			Polish	
Semester of study	5		ECTS credits			4.0	
Learning profile	general academic profile		Assessment form			assessment	
Conducting unit	Katedra Fizyki Teoretycznej i Informatyki Kwant. -> Faculty of Applied Physics and Mathematics -> Wydział Politechniki Gdańskiej						
Name and surname of lecturer (lecturers)	Subject supervisor		dr inż. Marcin Nowakowski				
	Teachers						
Lesson types	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	30.0	0.0	0.0	60
	E-learning hours included: 0.0						
	eNauczanie source address: https://enauczanie.pg.edu.pl/moodle/course/view.php?id=38564						
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	60		5.0		35.0	100
Subject objectives	The aim of this course is to acquaint students with the key concepts of modern cryptographic protocols, methods of information theory and coding theory applicable in cryptography and their applications in information processing.						
Learning outcomes	Course outcome		Subject outcome			Method of verification	
	[K6_K01] Understands the need to learn and improve professional and personal competencies. Can inspire and organize other people's learning process		Understands the need for lifelong learning. Can apply cryptographic algorithms to selected computer science problems.			[SK5] Ocena umiejętności rozwiązywania problemów występujących w praktyce	
	[K6_U02] Can analyze and solve simple scientific and technical problems, based on possessed knowledge, using analytical, numerical, simulation and experimental methods.		Has basic knowledge of the methodology and programming techniques for selected cryptologic issues.			[SU2] Ocena umiejętności analizy informacji	
	[K6_U03] Knows programming languages and can use basic software packages		Has basic knowledge in the field of cryptographic algorithms classification.			[SU1] Ocena realizacji zadania	
	[K6_W05] Has knowledge of programming methodology and techniques, and the use of selected IT tools in physics and technology.		Is able to analyze and solve simple technical problems in the area of cryptographic schemes.			[SW1] Ocena wiedzy faktograficznej	

Subject contents	Course content – lecture Symmetric cryptology: text cryptography: substitution algorithms. The quality of the cryptographic algorithm. Statistical cryptanalysis. Algorithms. Enigma: operation and cryptanalysis. Information theory and coding theory. Entrust quantities. Randomness. Linear codes. Block algorithms. DES algorithm. Algorithm's modes of operation. The quality of the DES algorithm. Cryptanalysis: differential and linear. Designing block algorithms, Feistel network. Combining block algorithms (TDES). Other block algorithms. Rijndael algorithm. Cryptographic protocols using symmetrical algorithms. Stream algorithms. Algorithm A5 (GSM). Pseudo-random strings. Analysis of stream ciphers. Asymmetric cryptography: key management. Diffie-Hellman algorithm. RSA algorithm. Quality of the RSA algorithm. TLS and SSL protocol. ElGamal algorithms and using elliptic curves. Other algorithms asymmetrical. Cryptographic protocols using unbalanced algorithms. One-way hash functions. MD5 and SHA function. Quality of unidirectional hash functions. The role of computational complexity and classes of computational problems. Advanced cryptographic protocols. Quarton cryptographic systems. Image cryptography. Artificial intelligence methods in cryptography. Quantum and post-quantum cryptography. The use of cryptography: patenting algorithms. Protection of transmitted and stored data in the electronic economy. The future of cryptology and other information protection techniques. Course content – laboratory 1. Implement the ECB, CBC, and FCB block cipher modes. Input: Text file to be encrypted. Output: Encrypted text file. Assumption: 64-bit blocks, use the text input function and transform into bit arrays. Any programming language: C#, Python, Java. 2. Implement a simplified version of the chosen cipher mode with one round of the DES algorithm. (Assumptions as above).		
Prerequisites and co-requisites	Discrete mathematics, Linear algebra, Probability theory. Knowledge of programming in object-oriented languages.		
Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	Exam	50.0%	50.0%
	Lab	50.0%	50.0%
Recommended reading	Basic literature	1. Jean-Philippe Aumasson, Nowoczesna kryptografia, PWN 2018. 2. Stinson D.R.: Kryptografia. W teorii i praktyce, WNT 2005. 3. B. Schneier Kryptografia dla praktykow, WNT 2002.	
	Supplementary literature	1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009. 2. D. Boneh, V. Shoup, A graduate course in applied cryptography, Stanford Univ., 2015	
	eResources addresses		
Example issues/ example questions/ tasks being completed	1. Implement ECB, CBC, FCB block encryption modes Input: The text file to be encrypted. Output: Encrypted text file. Assumption: 64 biotic blocks, use the text loading and transformation functions on bit arrays. Any programming language: C #, Python, Java ...		
	2. Implement the simplified version of the selected encryption mode from one round of the DES algorithm. (Assumptions as above).		
Practical activites within the subject	Not applicable		

Document generated electronically. Does not require a seal or signature.