



Subject card

Subject name and code	Cryptography, PG_00037330						
Field of study	Technical Physics						
Date of commencement of studies	October 2020		Academic year of realisation of subject		2021/2022		
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	2		Language of instruction		Polish		
Semester of study	4		ECTS credits		5.0		
Learning profile	general academic profile		Assessment form		exam		
Conducting unit	Department of Theoretical Physics and Quantum Information -> Faculty of Applied Physics and Mathematics						
Name and surname of lecturer (lecturers)	Subject supervisor		dr inż. Marcin Nowakowski				
	Teachers		dr inż. Marcin Nowakowski				
Lesson types and methods of instruction	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						
	Adresy na platformie eNauczanie:						
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		10.0		55.0	125
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_U03		Has basic knowledge in the field of programming methodology and techniques for selected cryptological problems.		[SU1] Assessment of task fulfilment		
	K6_U02		Can analyze and solve simple technical problems in the field of cryptographic schemes.		[SU2] Assessment of ability to analyse information		
	K6_K01		Understands the need for life-long learning. Can apply cryptographic algorithms for selected IT problems.		[SK5] Assessment of ability to solve problems that arise in practice		
	K6_W05		Has basic knowledge in the classification of cryptographic algorithms.		[SW1] Assessment of factual knowledge		

Subject contents	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. Quartion 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.		
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
	Lab	50.0%	50.0%
	Exam	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. <	