GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Cryptology, PG_00030022		
Field of study	Mathematics		
Date of commencement of studies	October 2022	Academic year of realisation of subject	2023/2024
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	blended-learning
Year of study	2	Language of instruction	Polish
Semester of study	3	ECTS credits	4.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Probability Theory and Biomathematics -> Faculty of Applied Physics and Mathematics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Jakub Maksymiuk	
	Teachers	dr inż. Jakub Maksymiuk mgr inż. Tomasz Gzella	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	30.0	0.0	15.0	15.0	0.0	60

E-learning hours included: 30.0

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	60	5.0	35.0	100

Subject objectives

Introduction to problems of modern cryptology. Presentation of a new area of applications of different branches of mathematics and conditions underlying their application.

Learning outcomes

Course outcome	Subject outcome	Method of verification
K7_U13	The student implements a project based on modern cryptological methods.	[SU4] Assessment of ability to use methods and tools
K7_W11	Student: - lists the criteria for assessing the quality of algorithms cryptographic - lists the basic concepts related to cryptology - explains the operation of basic symmetric and asymmetric algorithms - can, using appropriate tools, break simple ciphertexts	[SW1] Assessment of factual knowledge
K7_U08	The student uses the concepts of the theory of probability to cryptanalyze and assess the quality of cryptographic tools, e.g. random number generators	[SU1] Assessment of task fulfilment
K7_W08	Student knows the basic methods of cryptoanalsis and their limitations.	[SW3] Assessment of knowledge contained in written work and projects

Subject contents	Lecture: Introduction to cryptography: definitions, environment, books and conferences. Coding and ciphering. Cryptography till 1914. Military cryptology. Modern cryptology. Law and cryptology. Symmetric cryptography: ciphering of texts; substitution algorithms. The quality of an cryptographic algorithm. Statistical cryptanalysis. Transposition algorithms. Enigma: operation and cryptanalysis. Information theory and Shannon results. Ciphering of binary sequences. DES algorithm. DES modes of operation. Quality of DES algorithm. Differential and linear cryptanalysis of DES. Designing of block algorithms: Feistel network. Composition of block ciphers (TDES). Other block algorithms. AES algorithm (Rijndael). Simple cryptographic protocols with symmetric algorithms. Stream algorithms. A5 algorithm (GSM). Pseudorandom sequences. Cryptanalysis and design of stream ciphers. Asymmetric cryptography: key management. Diffie-Hellmann key exchange algorithm. RSA. algorithm. The quality of RSA algorithm. ElGamal algorithm and algorithms based on elliptic curves. Other asymmetric algorithms. Cryptographic protocols with asymmetric algorithms. Hash functions: definition. MD5 and SHA. Quality of hash functions. Advanced cryptographic protocols. Cryptography in real word: patents, Internet transactions. Future of cryptography. Laboratory: 1. Cryptool. ciphering of texts; substitution and transposition algorithms. 2. Cryptanalysis of substitution algorithms. Statistical characteristics of file with texts, source programs and executable programs. Coincidence and autocorrelation. 3. Cryptanalysis of Enigma. 4. Cryptography with modern symmetric algorithms. Differential cryptanalysis of DES 5. Cryptography with asymmetric algorithms. 6. Pseudorandom- and prime number. 7. Cryptanalysis of asymmetric algorithms. Project: Implementation of simple cryptographic algorithms or report about security of assigned algorithms or cryptographic protocols.
Prerequisites and co-requisites	Discrete mathematics, Linear algebra, Algebra, Probability theory

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Project	50.0%	60.0%
Practical exercise	50.0%	40.0%

Recommended reading	Basic literature
	1. Stinson D.R.: Cryptography. Theory and practice, CRC Press LLC, Third ed., 2005 2. Rubinstein-Salzedo S., Cryptography, Springer 2018
	Supplementary literature
	1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009 2. Paar C., Pelzl J., Understanding Cryptography, Springer 2010

	eResources addresses	Adresy na platformie eNauczanie: Kryptologia [Matematyka 2023/24] - Moodle ID: 28411 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=28411
Example issues/ example questions/ tasks being completed	Find the key used to encrypt the message encrypted using classic cipher. Discuss methods of attack on the ElGamal cryptosystem. Using differential cryptanalysis for two sets of plain texts and their ciphertexts find the set of potential keys.	
Work placement	Not applicable	