GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Cryptology, PG_00030022		
Field of study	Mathematics		
Date of commencement of studies	October 2023	Academic year of realisation of subject	2024/2025
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	2	Language of instruction	Polish
Semester of study	3	ECTS credits	5.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Divison of Nonlinear Analysis -> Institute of Applied Mathematics -> Faculty of Applied Physics and Mathematics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Jakub Maksymiuk	
	Teachers	mgr inż. Tomasz Gzella dr inż. Jakub Maksymiuk	

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: 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	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] Understands the mathematical foundations of the analysis of algorithms and computational processes, can construct algorithms with good numerical properties, used to solve typical and unusual mathematical problems.	The student implements a project based on modern cryptological methods.	[SU4] Assessment of ability to use methods and tools
[K7_W08] Knows advanced computation techniques, supporting the work of a mathematician and understand their limitations.	The student knows the basic methods cryptanalysis and its limitations	[SW1] Assessment of factual knowledge
[K7_W11] Knows the mathematical foundations of information theory, the theory of algorithms and cryptography and their practical applications, i.a. in programming and computer science.	Student: - lists the criteria for assessing the quality of cryptographic algorithms - lists the basic concepts related to cryptology - explains the operation of basic symmetric and asymmetric algorithms - is able to break simple ciphertexts using appropriate tools	[SW1] Assessment of factual knowledge
[K7_U08] Knows probability distributions and their properties; is able to use them in practical issues, is familiar with the basics of statistics (estimation issues and hypothesis testing) and the basics of statistical data processing.	The student applies the concepts and theorems of probability theory to cryptanalysis and quality assessment of cryptographic random number generators	[SU1] Assessment of task fulfilment

Subject contents

Lecture:

Introduction: definitions, environment, literature, coding and encryption. History to 1914. History of modern cryptology. Military and diplomatic cryptology. Legal aspects of cryptology application.

Symmetric cryptology: text cryptography: substitution algorithms. Quality of cryptographic algorithm. Statistical cryptanalysis. Transposition algorithms. Information theory and Shannon's results. Block algorithms. DES algorithm. Algorithm operating modes. Quality of DES algorithm. Design of block algorithms, Feistel network. Combining block algorithms (TDES). Other block algorithms. Rijndael algorithm. Simple cryptographic protocols using symmetric algorithms.

Stream algorithms. A5 algorithm (GSM). Pseudorandom sequences. Analysis of stream ciphers.

Asymmetric cryptography: key management. Diffie-Hellman algorithm. RSA algorithm. RSA algorithm quality. ElGamal and elliptic curve algorithms.

One-way hash functions: definition. MD5 and SHA functions. Quality of one-way hash functions

Advanced cryptographic protocols.

Application of cryptography: Protection of transmitted and stored data in electronic economy. The future of cryptology and other information protection techniques.

Laboratory and project:

- Text cryptography. Substitution and transposition ciphers.

- Cryptanalysis of substitution ciphers. Statistics of occurrence of characters in text files in Polish and English,

- Cryptography using modern symmetric algorithms.

- Cryptography using asymmetric algorithms.

- Pseudorandom and prime numbers.

- Implementation of simple cryptological algorithms or a report on the quality analysis of the indicated algorithms

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
Practical exercise	50.0%	40.0%
Project	50.0%	60.0%

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 - Moodle ID: 39608 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=39608
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. For two sets of plain texts and their ciphertexts find the set of potential keys.	
Work placement	Not applicable	

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