GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Foundations of Cryptography, PG_00048249		
Field of study	Informatics		
Date of commencement of studies	February 2025	Academic year of realisation of subject	2024/2025
Education level	second-cycle studies	Subject group	Optional subject group Specialty 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 -> Wydziały Politechniki Gdańskiej		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Robert Janczewski	
	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.

<table>
<tr><td>Learning outcomes</td><td>
<table>
<tr><th>Course outcome</th><th>Subject outcome</th><th>Method of verification</th></tr>
<tr><td>[K7_W11] knows and understands, to an increased extent, the general principles of creation and development of forms of individual entrepreneurship and the economic, legal and other conditions of various types of activities related to the awarded qualification, including the principles of protection of industrial property and copyright law</td><td>Student learns about the legal and ethical conditions related to the use of cryptosystems.</td><td>[SW1] Assessment of factual knowledge</td></tr>
<tr><td>[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</td><td>Student learns how cryptosystems work.</td><td>[SU1] Assessment of task fulfilment</td></tr>
<tr><td>[K7_K02] is ready to provide critical evaluation of received content and to acknowledge the importance of knowledge in solving cognitive and practical problems</td><td>Student learns how to evaluate cryptosystems.</td><td>[SK5] Assessment of ability to solve problems that arise in practice</td></tr>
<tr><td>[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</td><td>Student implements basic cryptosystems.</td><td>[SU1] Assessment of task fulfilment</td></tr>
</table>
</td></tr>
<tr><td>Subject contents</td><td>Introduction to modern cryptography. Classical cryptography: transposition and substitution ciphers, permutations. Modular arithmetic and RSA. Finite fields and AES. Symmetric and asymmetric cryptography.</td></tr>
<tr><td>Prerequisites and co-requisites</td><td></td></tr>
<tr><td>Assessment methods and criteria</td><td>
<table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td></td><td>50.0%</td><td>33.0%</td></tr>
<tr><td></td><td>50.0%</td><td>33.0%</td></tr>
<tr><td></td><td>50.0%</td><td>34.0%</td></tr>
</table>
</td></tr>
<tr><td>Recommended reading</td><td>
<table>
<tr><td>Basic literature</td><td>D.R. Stinson: "Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications) 3rd Edition".</td></tr>
<tr><td>Supplementary literature</td><td>None.</td></tr>
<tr><td>eResources addresses</td><td>Adresy na platformie eNauczanie:
Podstawy kryptografii 2025 - Moodle ID: 45152
https://enauczanie.pg.edu.pl/moodle/course/view.php?id=45152</td></tr>
</table>
</td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td></td></tr>
<tr><td>Work placement</td><td>Not applicable</td></tr>
</table>

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