GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

| | | | |
|---|---|---|---|
| Subject name and code | Cryptology, PG_00069469 | | |
| Field of study | Mathematics | | |
| Date of commencement of studies | October 2025 | Academic year of realisation of subject | 2026/2027 |
| Education level | second-cycle studies | Subject group | Specialty subject group<br>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 | 4.0 |
| Learning profile | general academic profile | Assessment form | assessment |
| Conducting unit | Divison of Nonlinear Analysis -> Institute of Applied Mathematics -> Faculty of Applied Physics and Mathematics -> Faculties of Gdańsk University of Technology | | |
| Name and surname of lecturer (lecturers) | Subject supervisor | dr inż. Jakub Maksymiuk | |
| | Teachers | dr inż. Jakub Maksymiuk | |

**Lesson types**

| 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_U10] understands the mathematical foundations of the analysis of algorithms and computational processes, constructs algorithms with good numerical properties, used to solve typical and unusual mathematical problems | Student implements a project based on modern cryptological methods. | [SU3] Assessment of ability to use knowledge gained from the subject<br>[SU4] Assessment of ability to use methods and tools |
| [K7_W03] demonstrates knowledge advanced computation techniques, supporting the work of a mathematician and understand their limitations. | Student knows the basic methods cryptanalysis and its limitations | [SW1] Assessment of factual knowledge |
| [K7_U06] uses probability distributions and their properties in practical issues, is familiar with the basics of statistics and the basics of statistical data processing | Students applies the concepts and theorems of probability theory to cryptoloanalysis and quality assessment of CRNG | [SU3] Assessment of ability to use knowledge gained from the subject |
| [K7_W06] analyzes the mathematical foundations of information theory, the theory of algorithms and cryptography and their practical applications, i.a. in programming and computer science. | Student:<br>- lists the criteria for assessing the quality of cryptographic algorithms<br>- lists the basic concepts related to cryptology<br>- explains the operation of basic symmetric and asymmetric algorithms | [SW1] Assessment of factual knowledge |

<table>
<tr><td>Subject contents</td><td>Course content – lecture<br>Lecture:<br><br>Introduction: definitions, environment, literature, coding and encryption. History to 1914. History of modern cryptology. Military and diplomatic cryptology. Legal aspects of cryptology application.<br><br>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.<br><br>Stream algorithms. A5 algorithm (GSM). Pseudorandom sequences. Analysis of stream ciphers.<br><br>Asymmetric cryptography: key management. Diffie-Hellman algorithm. RSA algorithm. RSA algorithm quality. ElGamal and elliptic curve algorithms.<br><br>One-way hash functions: definition. MD5 and SHA functions. Quality of one-way hash functions<br><br>Advanced cryptographic protocols.<br><br>Application of cryptography: Protection of transmitted and stored data in electronic economy. The future of cryptology and other information protection techniques.<br><br>Laboratory and project:<br><br>- Text cryptography. Substitution and transposition ciphers.<br><br>- Cryptanalysis of substitution ciphers. Statistics of occurrence of characters in text files in Polish and English,<br><br>- Cryptography using modern symmetric algorithms.<br><br>- Cryptography using asymmetric algorithms.<br><br>- Pseudorandom and prime numbers.<br><br>- Implementation of simple cryptological algorithms or a report on the quality analysis of the indicated algorithms</td></tr>
<tr><td>Prerequisites and co-requisites</td><td>Discrete mathematics, Linear algebra, Algebra, Probability theory, Algorithms and data structures</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>Practical exercise</td><td>50.0%</td><td>40.0%</td></tr><tr><td>Project</td><td>50.0%</td><td>60.0%</td></tr></table></td></tr>
<tr><td>Recommended reading</td><td><table><tr><td>Basic literature</td><td>1. Stinson D.R.: Cryptography. Theory and practice, CRC Press LLC, Third ed., 2005<br>2. Rubinstein-Salzedo S., Cryptography, Springer 2018</td></tr><tr><td>Supplementary literature</td><td>1. Bard G.: Algebraic Cryptanalysis, Springer Verlag 2009<br>2. Paar C., Pelzl J., Understanding Cryptography, Springer 2010</td></tr><tr><td>eResources addresses</td><td></td></tr></table></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td>Find the key used to encrypt the message encrypted using classic cipher.<br><br>Discuss methods of attack on the ElGamal cryptosystem.<br><br>For two sets of plain texts and their ciphertexts find the set of potential keys.</td></tr>
<tr><td>Practical activites within the subject</td><td>Not applicable</td></tr>
</table>

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