University of Gdańsk

Subject card

| | | | |
|---|---|---|---|
| Subject name and code | Cryptography and Information Processing Systems Safety, PG_00179126 | | |
| Field of study | Informatics | | |
| Date of commencement of studies | October 2024 | Academic year of realisation of subject | 2025/2026 |
| Education level | Bachelor's studies | Subject group | Obligatory subject group in the field of study<br>Optional subject group |
| Mode of study | part-time studies | Mode of delivery | at the university |
| Year of study | 2 | Language of instruction | Polish |
| Semester of study | 4 | ECTS credits | 8.0 |
| Learning profile | academic | Assessment form | exam |
| Conducting unit | | | |
| Name and surname of lecturer (lecturers) | Subject supervisor | dr Andrzej Borzyszkowski | |
| | Teachers | mgr Mateusz Miotk<br>dr Andrzej Borzyszkowski | |

| Lesson types | 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 | | | | | | |

| 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 | 0.0 | 0.0 | 60 |

| | |
|---|---|
| Subject objectives | Introduction to the topic of security of IT systems, with particular emphasis on cryptographic methods.<br><br>Familiarizing with terminology in English. |

## Learning outcomes

| Course outcome | Subject outcome | Method of verification |
|---|---|---|
| [INFL3_W02] has knowledge of discrete mathematics and probabilistic methods and statistics | is aware of the possible threats while using computers and knows solutions<br><br>understands how asymmetric cryptography works, what an electronic signature is, what methods are used to verify the integrity of documents<br><br>understands what are the possibilities and limitations of modern cryptography<br><br>knows the basic cryptographic algorithms and protocols<br><br>knows the possible attacks on information processing system security | [SW4] test/exam - oral or written<br>[SW5] implementation of a problem task |
| [INFL3_U09] is able to assess the suitability of programming paradigms and tools for solving problems of various types | is able to assess the legality of various activities related to breaking ciphers | [SU4] test/exam - oral or written |
| [INFL3_U03] can design and analyze algorithms for their correctness and computational complexity using appropriate algorithmic techniques and data structures | can create a secure password, create an X.509 or PGP certificate, calculate a hash function, write programs for encryption and cryptanalysis in various cryptographic systems | [SU4] test/exam - oral or written<br>[SU5] implementation of a problem task |

## Subject contents

- Main concepts and assumptions, symmetric and asymmetric cryptography, classical ciphers.
- The concept of a perfectly secure cipher, one-time pad, random and pseudorandom numbers.
- Computational security of a cipher, pseudorandom generators, stream cipher, multiple encryption, non-deterministic ciphers. Resistance to chosen plaintext attack, chosen cryptogram attack.
- Pseudorandom functions and permutations. Block ciphers and their modes. Block ciphers in practice, DES, AES/Rijndael.
- Data integrity: MAC and hash functions, their properties, birthday attack. "Encrypt, then authenticate".
- Private key cryptography and public key cryptography. The idea of asymmetric cryptography, attack from the middle, authentication and signature, hybrid cipher.
- RSA cipher, definition, attacks, ElGamal cipher, chosen cryptogram attack, bit commitment. Digital signature schemes, in symmetric and asymmetric cryptography, RSA and its weaknesses, ElGamal and DSS scheme, use of hash in signature. Public key infrastructure.
- Blockchain technology.
- Keys. Cryptographic protocols, man-in-the-middle attack, replay attack, nonces, timestamps, denial-of-service attack, tickets, Kerberos.
- Elements of steganography.

## Prerequisites and co-requisites

## Assessment methods and criteria

| Subject passing criteria | Passing threshold | Percentage of the final grade |
|---|---|---|
| exam | 51.0% | 40.0% |
| labs | 51.0% | 60.0% |

## Recommended reading

| | |
|---|---|
| Basic literature | Andrzej Borzyszkowski, materials for the course available on the website. |
| Supplementary literature | 1. J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008.<br>2. W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall , 2005.<br>3. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008 |
| eResources addresses | |

## Example issues/ example questions/ tasks being completed

1. Can a small key space ensure the security of a cipher? Is a large key space a guarantee of the security? Justify..
2. What block cipher modes do you know? Discuss the advantages and disadvantages of the different modes.
3. List some differences between the public key infrastructure and the trust model used in PGP.

| | |
|---|---|
| Work placement | Not applicable |

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