#### card of course

|  |  |
| --- | --- |
| Subject name | Foundations of security and cryptography |

1. The placement of the subject in the study system

|  |  |
| --- | --- |
| 1.1. Field of study | Computer science |
| 1.2. Form and path of study | Full-time/Part-time |
| 1.3. Level of education | First-cycle studies |
| 1.4. Study profile | Practical |

|  |  |
| --- | --- |
| 1. 5. Specialty | Cybersecurity and computer forensics |
| 1.6. Subject Coordinator | Mgr inż. Piotr Janiec, Mgr Lech Daniel, Mgr Emil Tomczyk |

2. General characteristics of the subject

|  |  |
| --- | --- |
| 2.1. Belonging to a subject group | Optional/practical |
| 2.2. Number of ECTS | 5 |
| 2.3. Language of lectures | Polish |
| 2.4. Semesters in which the subject is taught | III |
| 2.5.Criteria for selecting course participants | For specializations: Cybersecurity and computer forensics |

1. Learning outcomes and course delivery
   1. Subject Objectives

|  |  |
| --- | --- |
| No. | Subject Objectives |
|
| C1 | Familiarization with the concepts and categories of information security. |
| C2 | Acquiring knowledge and skills in the mathematical and algorithmic foundations of cryptography. |
| C3 | Familiarization with the elements of cryptography: basic encryption techniques, applications of encryption techniques. Familiarization with classical ciphers of Caesar, Scytale, Vigenère and modern Enigma. |
| C4 | Introduction to the elements of cryptography: modern symmetric (DES, 3DES, AES) and asymmetric (RSA) algorithms and ciphers, and secure exchange of encryption keys using Diffie-Hellman. |
| C5 | Familiarization with the elements of cryptography: Hash functions, hybrid encryption, [steganography](https://puw.wspa.pl/mod/resource/view.php?id=131201) . |
| C6 | Cryptographic key management, PKI infrastructure, certificates. |
| C7 | Introduction to the use of cryptography in secure network services. |
| C8 | Acquiring skills in using encryption algorithms, data encryption and decryption methods, and crypto data analysis. |

* 1. Subject-specific learning outcomes, divided into knowledge , skills and competences , with reference to the directional learning outcomes

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Description of subject  learning outcomes | Reference to  directional effects  learning (symbols) | Method of implementation (mark "X") | | | |
| ST | | NST | |
| Classes at the University | Activities on  the platform | Classes at the University | Activities on  the platform |
| After passing the course, the student knows and understands **the knowledge** | | | | | | |
| W1 | The student knows the theoretical foundations and methods of encryption. | INF\_W11  INF\_W15​ | X |  |  | X |
| W2 | The student has general theoretical knowledge of encryption methods. | X |  |  | X |
| W3 | The student has general theoretical knowledge of the use of encryption and encryption keys. | X |  |  | X |
| W4 | The student has general theoretical knowledge of the importance of encryption technology. | X |  |  | X |
| W5 | The student has general theoretical knowledge of the importance of hiding data using steganography techniques. | X |  |  | X |
| W6 | The student has general theoretical knowledge of cryptographic key management, PKI infrastructure and certificates. | X |  |  | X |
| After passing the course, the student is **able** to: | | | | | | |
| U1 | The student is able to apply an encryption algorithm. | INF\_U11 INF\_U16 INF\_U25 | X |  | X |  |
| U2 | The student is able to apply data encryption and decryption methods. | X |  | X |  |
| U3 | The student is able to recognize specific methods of encrypting and decrypting data. | X |  | X |  |
| U4 | The student can hide data using steganography techniques. | X |  | X |  |
| U5 | The student is able to create and manage CA certificates. | X |  | X |  |
| After completing the course, the student is ready to take part in **social competences.** | | | | | | |
| K1 | Understands the need to update his/her knowledge of encryption mechanisms and is ready to convey it in an understandable manner. | INF\_K01 | X |  | X |  |
| K2 | Is able to convey acquired knowledge  in an understandable way. | X |  | X |  |

3.3. Forms of teaching and their number of hours - Full-time studies (ST), Part-time studies (NST)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Path | Lecture | Exercises | Design | Workshop | Laboratory | Seminar | Lecturer | Classes conducted using distance learning methods and techniques in the form of a lecture | Other | **ECTS points** |
| **ST** | 20 |  |  |  | 30 |  |  |  |  | 5 |
| **NST** |  |  |  |  | 20 |  |  | 10 |  | 5 |

3.4. Content of education (separately for each form of classes: (W, ĆW, PROJ, WAR, LAB, LEK, OTHER). It should be marked (X) how the given content will be implemented (classes at the university or classes on the e-learning platform conducted using distance learning methods and techniques)

TYPE OF CLASS: LECTURE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Content of the course | Reference to subject-specific learning outcomes | Method of implementation (mark "X") | | | |
| ST | | NST | |
| **Classes at the University** | **Activities on  the platform** | **Classes at the University** | **Activities on  the platform** |
| 1. | Basic concepts and categories of information security, Mathematical and algorithmic foundations of cryptography. | W1, W2 | X |  |  | X |
| 2. | Services related to information protection, categories of threats to IT systems. | W1, W2 | X |  |  | X |
| 3. | Elements of cryptography: basic encryption techniques, applications of encryption techniques. | W1, W2, W3 | X |  |  | X |
| 4. | Classical algorithms and ciphers: Caesar, Scytale, Vigenère. Modern ciphers: Enigma. | W1, W2, W3 | X |  |  | X |
| 5. | Symmetric algorithms and ciphers: DES, 3DES, AES. | W2, W3, W4 | X |  |  | X |
| 6. | Asymmetric ciphers and algorithms: RSA, El-Gamal. Secure encryption key exchange using Diffie-Hellman. | W2, W3, W4 | X |  |  | X |
| 7. | Hash functions: SHA, MD5. Steganography. | W1, W2, W3, W4, W5 | X |  |  | X |
| 8. | Authentication and digital signatures. Electronic signature. | W1, W2, W3, W4 | X |  |  | X |
| 9. | Cryptographic key management, PKI infrastructure, certificates. | W1, W2, W3, W4, W6 | X |  |  | X |
| 10. | Summary of classes and discussion of grades. |  | X |  |  | X |

TYPE OF CLASS: LABORATORY

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No. | Content of the course | Reference to subject-specific learning outcomes | Method of implementation (mark "X") | | | |
| ST | | NST | |
| **Classes at the University** | **Activities on  the platform** | **Classes at the University** | **Activities on  the platform** |
| 1. | Lab – Ex 1. Caesar Cipher.  Ex 2. Breaking the Caesar Cipher. Ex 3. The Scytale Cipher and breaking the Scytale cipher. | U1, U2, U3, K1, K2 | X |  | X |  |
| 2. | Lab – Lab 1. The Vigenère Cipher and breaking the cipher. Lab 2. The Columnar Cipher and breaking the cipher. Lab 3. The ADFGVX Cipher and breaking the cipher. | U1, U2, U3, K1, K2 | X |  | X |  |
| 3. | Laboratory – Ex 1. The Enigma Cipher. Ex 2. Crypto analysis, cipher breaking. Enigma Ex 3. British Typex Cipher Machine and cipher breaking. Ex 4. German SZ42 Cipher and cipher breaking. | U1, U2, U3, K1, K2 | X |  | X |  |
| 4. | Laboratory – Modern Block Ciphers. Lab 1. DES Cipher. Lab 2. RC4 and DES Ciphers - ECB vs CBC. Lab 3. Examination of the entropy of the DES cipher and breaking the DES cipher using the Brute-Force method. | U1, U2, U3, K1, K2 | X |  | X |  |
| 5. | Laboratory – Modern Block Ciphers. Cl1 - AES Cipher - Advanced Encryption Standard - explanation of operation and keys Cl 2. AES Cipher - File Encryption. Cl 3. AES Cipher - Text Encryption Using AES and PKCS#5. | U1, U2, U3, K1, K2 | X |  | X |  |
| 6. | Laboratory – Lab 1. Modern ciphers – Perfect Ciphers and the disposable One-Time Pad. | U1, U2, U3, K1, K2 | X |  | X |  |
| 7. | Lab - Modern Asymmetric Ciphers. Lab 1. RSA Asymmetric Cipher. Lab 2. RSA Asymmetric Cipher - Let's Try to Break It Using Factorization. Lab 3. Secure Exchange of Encryption Keys Using Diffie-Hellman. | U1, U2, U3, K1, K2 | X |  | X |  |
| 8. | Lab - Modern Ciphers - Lab 1. Hash Functions. Lab 2. Hybrid Encryption using Symmetric AES and Asymmetric RSA Ciphers. Lab 3. Let's create a secure AES encrypted video chat, with secure key exchange using Diffie-Hellman. | U1, U2, U3, K1, K2 | X |  | X |  |
| 9. | Laboratory - Modern Ciphers - Steganography Cl 1. Hiding data in text. Cl 2. Hiding data in an image. Cl 3. Hiding data in an image and cracking passwords. | U1, U2, U3, U4, K1, K2 | X |  | X |  |
| 10. | Lab - Cryptographic Key Management, Certificates – Lab 1. Checksum Functions Using OpenSSL. Lab 2. Encryption and Decryption Using OpenSSL. Lab 3. Private CA Certificate Authority Using OpenSSL. | U1, U2, U3, U5, K1, K2 | X |  | X |  |
| 11. | Summary of classes and discussion of grades. |  | X |  | X |  |

3.5. Methods of verifying learning outcomes (indication and description of methods of conducting classes and verification of achievement of learning outcomes and method of documentation)

|  |  |  |  |
| --- | --- | --- | --- |
| Subject Effects | Teaching methods | Methods of verifying learning outcomes | Documentation methods |
| KNOWLEDGE | | | |
| W1-W6 | Lecture using multimedia. | Lecture - graded (on the platform) in the form of a knowledge test. | Test archived on the platform. |
| SKILLS | | | |
| U1-U5 | Solving tasks, performing exercises. | Laboratory - practical tasks performed in the laboratory. The final grade is a weighted average. | Task files on the platform. |
| SOCIAL COMPETENCES | | | |
| K1-K2 | Solving tasks, performing exercises. | Laboratory - practical tasks performed in the laboratory. The final grade is a weighted average. | Task files on the platform. |

3.6. Assessment criteria for the achieved learning outcomes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Learning effect | For a grade of 3 or "pass."  the student knows and understands/is able to/is ready to | For a grade of 3.5, the student knows and understands/is able to/is ready to | For a grade of 4, the student knows and understands/is able to/is ready to | For a grade of 4.5, the student knows and understands/is able to/is ready to | For a grade of 5, the student knows and understands/is able to/is ready to |
| W | 51-60% of knowledge indicated in learning outcomes | 61-70% of knowledge indicated in learning outcomes | 71-80% of knowledge indicated in learning outcomes | 81-90% of knowledge indicated in learning outcomes | 91-100% of knowledge indicated in learning outcomes |
| U | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |
| K | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |

3.7. Literature

**Basic**

1. „Nowoczesna kryptografia” – Jean Philippe Amuasson - Helion 2018
2. Piper Fred, Murphy Sean, Kryptografia, Wydawnictwo Naukowe PWN, Warszawa, 2022

**Supplementary**

1. „Bezpieczeństwo systemów informatycznych” - William Stallings, Lawrie Brown, Helion 2019
2. Stinson Douglas R., Paterson Maura B., Kryptografia: w teorii i praktyce, Wydawnictwo Naukowe PWN, Warszawa, 2021

4. Student workload - ECTS points balance

|  |  |  |
| --- | --- | --- |
| **Types of student activity** | **Student Load** | |
| **ST** | **NST** |
| **Classes requiring direct contact between the student and the academic teacher at the university premises** | **50** | **30** |
| Classes included in the study plan | 50 | 30 |
| **Student's own work** | **75** | **95** |
| Ongoing preparation for classes, preparation of project work/presentations/etc. | 35 | 45 |
| Preparation for passing classes | 40 | 50 |
| **TOTAL STUDENT HOURLY LOAD** | **125** | **125** |
| **Number of ECTS points** | **5** | **5** |

|  |  |
| --- | --- |
| Last change date | 30/09/2024 |
| The changes were introduced | INF Education Quality Team |
| The changes were approved | Arkadiusz Gwarda, M.A. |