Appendix No. 1.5 to the Resolution No. 61/2025
of the Rector of the University of Rzeszów

SYLLABUS

REGARDING THE QUALIFICATION CYCLE FROM 2026 TO 2029
ACADEMIC YEAR 2028/2029

1. BASIC COURSE/MODULE INFORMATION

Course/Module title	Basics of Cryptography
Course/Module code *	
Faculty (name of the unit offering the field of study)	Faculty of Exact and Technical Sciences
Name of the unit running the course	Institute of Mathematics
Field of study	Mathematics
Qualification level	First-cycle studies (Bachelor's)
Profile	Specialisation course
Study mode	Full-time
Year and semester of studies	Year 3, Semester 6
Course type	Major subject
Language of instruction	English
Coordinator	Andrzej Łopuszański, PhD, DSc
Course instructor	Andrzej Łopuszański, PhD, DSc

* - as agreed at the faculty

1.1.Learning format – number of hours and ECTS credits

Semester (no.)	Lectures	Classes	Laboratories	Seminars	Practical classes	Internships	others	**ECTS credits**
6	30		30					6

1.2. Course delivery methods

☒ conducted in a traditional way

☐ involving distance education methods and techniques

1.3. Course/Module assessment (exam, pass with a grade, pass without a grade)

Lecture – exam, laboratories – pass with a grade

2.PREREQUISITES

Elements of probability theory, combinatorics and statistics, algebra and number theory.

3. OBJECTIVES, LEARNING OUTCOMES, CURRICULUM CONTENT AND TEACHING METHODS USED

3.1 Course objectives

O1	The aim of the course is to familiarize students with the subject of cryptography.

3.2 Learning outcomes for the subject

Learning Outcome	The description of the learning outcome defined for the course/module	Relation to the degree programme outcomes
LO_01	The student knows and understands the basic concepts of cryptology and cryptanalysis, and also has knowledge of information theory, computational complexity theory and number theory necessary as a basis for cryptography.	K_W07
LO_02	The student knows the history of cryptography and its development.	K_W08
LO_03	The student knows and understands how the most important symmetric and asymmetric cryptography algorithms work.	K_W07
LO_04	The student knows the tools and protocols that use cryptographic algorithms in a practical way.	K_W07
LO_05	The student is able to create and implement an encryption algorithm.	K_U16,K_U22
LO_06	The student is able to encrypt and decrypt in a given cryptographic system.	K_U16,K_U22
LO_07	The student is able to use various cryptanalysis methods.	K_U16,K_U22
LO_08	The student is aware of the need to ensure information security and confidentiality. They are familiar with the characteristics of existing cryptographic tools and algorithms and can select them based on their needs and application area.	K_K04,K_K05,K_K07

3.3. Course content (to be completed by the coordinator)

A. Lectures

Content outline
Introduction to cryptography. Basic concepts of cryptography and cryptanalysis. The difference between coding and encryption. Cryptography and steganography. Classification and discussion of attacks on cryptographic systems. Methods of information secrecy in the past. The history (up to the 19th century) and development of cryptography and cryptanalysis. The simplest historical cryptographic systems. Their vulnerabilities and attack examples. Substitution and transposition ciphers. Letter frequency analysis. Types of BruteForce and HillClimbing attacks. Affine (e.g., Caesar, atbash), simple replacement, and homophonic (e.g.,) substitution ciphers, their weaknesses and vulnerabilities, and types of effective attacks against them. Formal definition of a cryptographic system. A probabilistic Markov approach to cryptanalysis. Shannon information theory: information quantity, message entropy, language redundancy. Theoretical security of a cryptographic system. Computational complexity of the Kolmogorov algorithm. Security of a cryptographic system from the perspective of computational complexity theory. Practical security of cryptographic systems. Polyalphabetic substitution ciphers (e.g., Vigenere and its variations: Beaufort, autokey). Linear algebra modulo N and matrix calculus modulo N. Polygraphic substitution ciphers (Playfair, bifid, trifid, Hill), their weaknesses and sensitivities, Kasiski's method for Vigenere. Block ciphers. Transposition ciphers with historical examples (including RailFence, Path, Kardano Grill, Columnar Transposition, etc.), their weaknesses and vulnerabilities, and effective attacks against them. The fractionation method as an effective way of combining ciphers. Double transposition cipher, VIC cipher. Symmetric cryptography algorithms. Stream and block algorithms. DES, Blowfish, and AES algorithms. Asymmetric cryptography algorithms. Public-key cryptography. Public key and private key. RSA and ElGamal. Hash functions and message authentication codes. Message integrity and non-repudiation. Hash functions. Conflict-free hash functions. MD5 and SHA-1 algorithms. MAC message authencation codes.

B. Classes, laboratories, seminars, practical classes

Content outline
Python implementation of historical ciphers of simple substitution, columnar transposition, Vigener, Playfair, Hill, and others. Implementation of various attacks on the above-mentioned and other sensitive types of historical ciphers (in class and in group or individual projects for more independent work). Introduction to code efficiency, which is important for cryptanalysis, and comparisons. Implementation of fractionation using simple substitution and transposition as an example.

3.4 Teaching methods

Laboratory exercises: computer work, practical project

Lecture: lecture with multimedia presentation

4. Assessment techniques and criteria

4.1 Methods of evaluating learning outcomes

Learning outcome	Methods of assessment of learning outcomes (e.g. test, oral exam, written exam, project, report, observation during classes)	Learning format (lectures, classes,...)
LO-01	observation during classes, project and test	lectures, laboratories
LO-02	observation during classes, project and test	lectures, laboratories
LO-03	observation during classes, project and test	lectures, laboratories
LO-04	observation during classes, project and test	lectures, laboratories
LO-05	observation during classes, project and test	lectures, laboratories
LO-06	observation during classes, project and test	lectures, laboratories
LO-07	observation during classes, project and test	lectures, laboratories
LO-08	observation during classes	lectures, laboratories

4.2 Conditions for passing the course (assessment criteria)

Laboratory: project at the end of the semester (graded depending on the chosen difficulty level) taking into account work during the semester.
Lecture: Exam:
a minimum of 50% is required to pass. Final grade according to the scale:
below 50% – fail,
[50–60%) – satisfactory,
[60–70%) – satisfactory plus,
[70–80%) – good,
[80–90%) – good plus,
[90–100%] – very good

5. Total student workload needed to achieve the intended learning outcomes – number of hours and ECTS credits

Activity	Number of hours
Course hours	60
Other contact hours involving the teacher (consultation hours, examinations)	5
Non-contact hours - student's own work (preparation for classes or examinations, projects, etc.)	85
Total number of hours	150
Total number of ECTS credits	6

* One ECTS point corresponds to 25-30 hours of total student workload

6. Internships related to the course/module

Number of hours	*Not applicable*
Internship regulations and procedures	*Not applicable*

7. Instructional materials

Compulsory literature:
1. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography (wydanie 2), CRC Press (Taylor & Francis Group), 2015.
2. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, 2010.
3. Douglas Stinson, Cryptography: Theory and Practice, Chapman and Hall / CRC, 2005.
4. Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2018.

Complementary literature:
1. William Stallings, Cryptography and Network Security: Principles and Practice (wydanie 5), Prentice Hall, 2011.
2. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, Inc., 2010.
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
4. Wade Trappe, Lawrence Washington, Introduction to Cryptography with Coding Theory (wydanie 2), Prentice Hall, 2005.

Approved by the Head of the Department or an authorised person