COURSE DESCRIPTION CARD - SYLLABUS

Course name
Multimedia protection techniques [S1Cybez1>TOMm]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr hab. inż. Dawid Mieloch prof. PP
dawid.mieloch@put.poznan.pl

mgr inż. Jakub Stankowski
jakub.stankowski@put.poznan.pl

Lecturers

Prerequisites

Basic knowledge of the basics of programming, digital technology, multimedia signal processing and the ability to obtain information from indicated sources, including sources in English.

Course objective

Provide basic knowledge on steganography, watermarking, multimedia encryption, multimedia access control, quantum cryptography and apply quantum encryption.

Course-related learning outcomes

Knowledge:
K1_W12 - Has in-depth knowledge of authentication, authorization, and access control principles for computer systems; is aware of the necessity of applying access control policies and adapting them to the level of risk; knows the principles of biometric authentication.
K1_W13 - Knows the principles of data hiding, i.e., cryptography and steganography; has advanced

knowledge of cryptography, cryptographic algorithms, their limitations, and their significance for cybersecurity; has extended knowledge of data compression.

Skills:
K1_U01 - Able to use literature sources, integrate acquired information, evaluate and interpret it and draw conclusions, in order to solve complex and unusual problems in the area of cyber security.
K1_U08 - Can compare different technical solutions, evaluate them in terms of selected utility, economic, ecological, legal and ethical criteria

Social competences:
K1_K05 - Is aware of the importance of own work and the need to comply with the principles of professional ethics, is ready to comply with the rules of teamwork and bear responsibility for jointly implemented tasks, as well as care for the achievements and traditions of the profession

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture - written exam, closed question (test)/open question,
Laboratories - the final grade consists of: substantive evaluation of the performance of laboratory tasks, continuous evaluation, at each class (oral answers), ongoing activity in class, grades obtained on written tests, obtaining additional points for activity during the class and the results of tasks for independent execution.
Grading scale: p<50% : 2.0; p∈<50%, 60%) : 3.0; p∈<60%, 70%) : 3.5; p∈<70%, 80%) : 4.0; p∈<80%, 90%)
: 4.5; p >= 90% : 5.0
The course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The program content covers topics related to the protection, analysis, and access control of multimedia in the context of security. It includes methods for hiding information in audiovisual files, watermarking techniques for identifying content sources, and encryption mechanisms used to protect files from unauthorized access. Particular emphasis is placed on methods for detecting manipulations and analyzing multimedia integrity, which are crucial for identifying forgeries and safeguarding data from tampering.
Additionally, the program content addresses issues related to access control for digital content, including systems that restrict copying and distribution of multimedia. Modern security technologies are also discussed, including cryptographic methods and their impact on the quality and efficiency of data transmission. The relationship between compression and content security is explored, along with the use of advanced techniques to ensure the integrity and confidentiality of multimedia in digital environments.

Course topics

1. Hiding information in multimedia
• Basic concepts and objectives.
• Methods for embedding hidden data in audio, image, and video files.
• Applications of data hiding in the context of privacy protection and security.
• Techniques for detecting hidden data in multimedia, including statistical and visual analysis.
2. Multimedia watermarking techniques
• Types of watermarking and their applications.
• Methods for embedding watermarks in different multimedia formats.
• Techniques for removing and modifying watermarks.
• Examples of attacks on watermarked content and protection methods.
3. Encryption of multimedia content
• Methods for securing audiovisual data.
• Encryption algorithms and their impact on content quality.
• Mechanisms for protecting multimedia during storage and transmission.

• Efficiency of encryption in content distribution systems.
• The impact of compression methods on the security of encrypted files.
4. Access protection for multimedia
• Access control mechanisms and their role in content security.
• Methods for restricting copying and playback.
• Examples of multimedia protection systems in practice.
• Privacy issues and limitations related to content protection.
5. Modern methods for protecting multimedia data
• Utilization of new technologies for securing information.
• Key distribution methods and protection against data interception.
• Examples of applications in communication, cloud computing, and smart systems.

Teaching methods

Hybrid lecture: traditional lecture with the addition of multimedia educational materials, problem lectures - case analysis, it is allowed to invite speakers from industry or science
Laboratory - computer classes.

Bibliography

Basic:
Deb, S., & Sahu, A. K. (2023). Securing the Digital World: A Comprehensive Guide to Multimedia Security. Routledge.
Puech, W. (2023). Multimedia Security 1: Authentication and Data Hiding. Wiley-ISTE.
Anderson, R. (2020). Inżynieria zabezpieczeń. Tom II. Helion.
Pieprzyk, J. (2011). Teoria bezpieczeństwa systemów komputerowych. Helion.

Additional:
Wong, D. (2023). Prawdziwy świat kryptografii. Helion.
Aumasson, J.-P. (2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press.
Baker, R. L. (2024). Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence. Helion.

Breakdown of average student's workload

	Hours	ECTS
Total workload	78	3,00
Classes requiring direct contact with the teacher	48	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00