GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Information Systems Security, PG_00048305		
Field of study	Electronics and Telecommunications		
Date of commencement of studies	February 2023	Academic year of realisation of subject	2023/2024
Education level	second-cycle studies	Subject group	Obligatory subject group in the field of study 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	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Teleinformation Networks -> Faculty of Electronics, Telecommunications and Informatics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Bartosz Czaplewski	
	Teachers	mgr inż. Remigiusz Martyniak dr inż. Bartosz Czaplewski	

Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	30.0	0.0	15.0	0.0	0.0	45
	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	45	3.0	27.0	75

Subject objectives	Knowledge of information security threats and methods of information protection against these threats.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K7_W08] Knows and understands, to an increased extent, the fundamental dilemmas of modern civilisation, the main development trends of scientific disciplines relevant to the field of education.	The student understands and identifies the challenges related to the distribution of keys, the creation of a secure channel, the resistance of asymmetric cryptography to the operation of quantum computers. The student knows and understands how critical it is for modern civilization to maintain an appropriate level of information security.	[SW1] Assessment of factual knowledge
[K7_U07] can apply advanced methods of process and function support, specific to the field of study	Student understands, identifies and classifies the methods of symmetric cryptography, asymmetric cryptography, steganography, digital fingerprinting.	[SU2] Assessment of ability to analyse information [SU4] Assessment of ability to use methods and tools
[K7_U06] can analyse the operation of components, circuits and systems related to the field of study; measure their parameters; examine technical specifications; interpret obtained results and draw conclusions	The student is able to run, measure and analyse the most important symmetric and asymmetric encryption algorithms.	[SU2] Assessment of ability to analyse information [SU4] Assessment of ability to use methods and tools
[K7_W03] Knows and understands, to an increased extent, the construction and operating principles of components and systems related to the field of study, including theories, methods and complex relationships between them and selected specific issues - appropriate for the curriculum.	Student identifies, classifies and recognizes threatens of information security during data transmission and basic cryptographic systems. Student identifies and classifies security services and mechanisms.	[SW1] Assessment of factual knowledge
[K7_W06] Knows and understands, to an increased extent, the basic processes taking place in the life cycle of devices, facilities and technical systems.	Student analyses encryption and decryption processes as well as estimates cryptographic system resistance to malicious attacks.	[SW1] Assessment of factual knowledge

Subject contents

1. Information system security
2. Basic information security aspects
3. Network security model
4. Basic aspects of cryptographic systems
5. Cryptanalysis methods
6. Classic ciphers
7. Introduction to block ciphers
8. Data Encryption Standard (DES)
9. Design principles for block ciphers
10. Block cipher modes
11. Double and triple encryption (3DES)
12. International Data Encryption Algorithm (IDEA)
13. Advanced Encryption Standard (AES)
14. Link encryption and end-to-end encryption
15. Key distribution methods
16 Generating pseudo-random numbers
17. RC4 stream cipher
18. Asymmetric cryptographic systems
19. RSA system
20. Distribution of public keys
21. Diffie-Hellman algorithm
22. ElGamal algorithm
23. Elliptic-curve cryptography
24. The future of asymmetric cryptography
25. Asymmetric cryptography resistant to attacks of quantum computers
26. Message authentication
27. One-way hash functions
28. Rainbow tables
29. Digital Signature properties
30. Digital Signature Algorithm (DSA)
31. The basics of steganography
32. Digital fingerprinting
33. Reversible Data Hiding

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
final test	50.0%	60.0%
measurement reports	50.0%	40.0%

Recommended reading	Basic literature	B. Schneier, Kryptografia dla praktyków, WN-T, Warszawa 2004 J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2010 N. Ferguson,B. Schneier, Kryptografia w praktyce, Helion, 2004 W. Stallings, Cryptography and Network Security, Principles and Practice, Fourth Edition, Prentice Hall, 2005 M. Stamp, Information Security: Principles and Practice, J. Wiley, 2011
	Supplementary literature	B. Czaplewski, Nowe metody łącznego fingerprintingu i deszyfracji do zabezpieczania obrazów kolorowych, rozprawa doktorska, WETI PG, 2015Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, B. Ma, Reversible Data Hiding: Advances in the Past Two Decades, IEEE Access, 2016
	eResources addresses	Adresy na platformie eNauczanie: Bezpieczeństwo Systemów Informacyjnych 2023/2024 - Moodle ID: 31587 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=31587
Example issues/ example questions/ tasks being completed	none	
Work placement	Not applicable	