GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Information Systems Security, PG_00055353						
Field of study	Electronics and Telecommunications						
Date of commencement of studies	October 2026		Academic year of realisation of subject	2026/2027			
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	1		Language of instruction	English			
Semester of study	2		ECTS credits	3.0			
Learning profile	general academic profile		Assessment form	assessment			
Conducting unit	Department of Teleinformation Networks -> Faculty of Electronics Telecommunications and Informatics -> Faculties of Gdańsk University of Technology						
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Bartosz Czaplewski					
	Teachers	dr inż. Bartosz Czaplewski Vorya Waladi					

Lesson types	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_U09] can carry out a critical analysis of the functioning of existing technical solutions and assess these solutions, as well as apply experience related to the maintenance of advanced technical systems, devices and facilities typical for the field of studies, gained in the professional engineering environment	The student is able to run, measure and analyze the most important symmetric and asymmetric encryption algorithms. The student analyzes encryption and decryption processes and assesses the resistance of cryptographic systems to attacks.	[SU3] Assessment of ability to use knowledge gained from the subject [SU2] Assessment of ability to analyse information
	[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_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

Subject contents	Course content – lecture 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	

<table>
<tr><td>Assessment methods and criteria</td><td colspan="2"><table>
<tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr>
<tr><td>measurement reports</td><td>50.0%</td><td>40.0%</td></tr>
<tr><td>final test</td><td>50.0%</td><td>60.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Recommended reading</td><td>Basic literature</td><td>B. Schneier, Kryptografia dla praktyków, WN-T, Warszawa 2004J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2010N. Ferguson,B. Schneier, Kryptografia w praktyce, Helion, 2004W. Stallings, Cryptography and Network Security, Principles and Practice, Fourth Edition, Prentice Hall, 2005M. Stamp, Information Security: Principles and Practice, J. Wiley, 2011</td></tr>
<tr><td>Supplementary literature</td><td>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</td></tr>
<tr><td>eResources addresses</td><td></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td colspan="2">none</td></tr>
<tr><td>Practical activites within the subject</td><td colspan="2">Not applicable</td></tr>
</table>

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