



## Subject card

Subject name and code	Information Systems Security, PG_00055353						
Field of study	Electronics and Telecommunications						
Date of commencement of studies	October 2022		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	4		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		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_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.	[SU4] Assessment of ability to use methods and tools [SU2] Assessment of ability to analyse information
	[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 threats of information security during data transmission and basic cryptographic systems. Student identifies and classifies security services and mechanisms.	[SW1] Assessment of factual knowledge
	[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_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.	[SU4] Assessment of ability to use methods and tools [SU2] Assessment of ability to analyse information
	[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	<ol style="list-style-type: none"> <li>1. Information system security</li> <li>2. Basic information security aspects</li> <li>3. Network security model</li> <li>4. Basic aspects of cryptographic systems</li> <li>5. Cryptanalysis methods</li> <li>6. Classic ciphers</li> <li>7. Introduction to block ciphers</li> <li>8. Data Encryption Standard (DES)</li> <li>9. Design principles for block ciphers</li> <li>10. Block cipher modes</li> <li>11. Double and triple encryption (3DES)</li> <li>12. International Data Encryption Algorithm (IDEA)</li> <li>13. Advanced Encryption Standard (AES)</li> <li>14. Link encryption and end-to-end encryption</li> <li>15. Key distribution methods</li> <li>16. Generating pseudo-random numbers</li> <li>17. RC4 stream cipher</li> <li>18. Asymmetric cryptographic systems</li> <li>19. RSA system</li> <li>20. Distribution of public keys</li> <li>21. Diffie-Hellman algorithm</li> <li>22. ElGamal algorithm</li> <li>23. Elliptic-curve cryptography</li> <li>24. The future of asymmetric cryptography</li> <li>25. Asymmetric cryptography resistant to attacks of quantum computers</li> <li>26. Message authentication</li> <li>27. One-way hash functions</li> <li>28. Rainbow tables</li> <li>29. Digital Signature properties</li> <li>30. Digital Signature Algorithm (DSA)</li> <li>31. The basics of steganography</li> <li>32. Digital fingerprinting</li> <li>33. Reversible Data Hiding</li> </ol>		
Prerequisites and co-requisites			

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	measurement reports	50.0%	40.0%
	final test	50.0%	60.0%
Recommended reading	Basic literature	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	
	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: Information Systems Security 2023/2024 - Moodle ID: 31589 <a href="https://enauczanie.pg.edu.pl/moodle/course/view.php?id=31589">https://enauczanie.pg.edu.pl/moodle/course/view.php?id=31589</a>	
Example issues/ example questions/ tasks being completed	none		
Work placement	Not applicable		