GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Data Security in Radio Communication Systems, PG_00047470
Field of study	Electronics and Telecommunications

Date of commencement of studies	February 2025	**Academic year of realisation of subject**	2025/2026
Education level	second-cycle studies	**Subject group**	Optional subject group Specialty subject group 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**	2.0
Learning profile	general academic profile	**Assessment form**	assessment

Conducting unit	Department of Radiocommunication Systems and Networks -> Faculty of Electronics, Telecommunications and Informatics
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Andrzej Marczak
	Teachers	dr inż. Andrzej Marczak

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	15.0	0.0	15.0	0.0	0.0	30
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	30	4.0	16.0	50

Subject objectives	The aim of the course is teach students the cryptographic security methods in radiocommunication systems.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K7_K02] is ready to provide critical evaluation of received content and to acknowledge the importance of knowledge in solving cognitive and practical problems	The student is able to choose the right methods of data protection for appropriate applications.	[SK5] Assessment of ability to solve problems that arise in practice
[K7_U07] can apply advanced methods of process and function support, specific to the field of study	The student is able to use the acquired knowledge of cryptographic data protection methods to understand the methods of data protection used in radio communication systems.	[SU1] Assessment of task fulfilment
[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	The student knows and understands the role of individual blocks in the diagrams depicting the method of data security in radio communication systems.	[SW1] Assessment of factual knowledge

Subject contents	1. Basic ideas and targets of data security. 2. Block ciphers (DES, AES, Kasumi). 3. Stream ciphers, stream cipher's keys generation. 4. Asymmetric ciphers. 5. Message Authentication Codes (MAC). 6. Threats for data security in radio communication systems. 7. Authentication and ciphering in radio communication systems. 8. Transmission security in TETRA trunked radio system. 9. Transmission security in CDMA2000 networks. 10. Transmission security in GSM. 11. Transmission security in UMTS. 12. Transmission security in IEEE802.11. 13. Mechanisms of security in Bluetooth. 14. Mechanisms of security in WIMAX. 15. Software Defined Radio – data security aspects		
Prerequisites and co-requisites			

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	Written exam	51.0%	90.0%
	Practical exercise	50.0%	10.0%

Recommended reading	Basic literature	V.Niemi, K.Nyberg: UMTS Security, John Wiley & Sons Inc. B. Preneel "Mobile and Wireless Communications Security" In *NATO ASI on Aspects of Network and Information Security*, IOS Press P. Chandra "Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security", Elsevier Inc 2005
	Supplementary literature	Roger J. Sutton: Secure Communications: Applications and Management, John Wiley & Sons Inc.
	eResources addresses	Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed	
Work placement	Not applicable

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