GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Cryptography in Cyber Security, PG_00048039		
Field of study	Informatics		
Date of commencement of studies	February 2023	Academic year of realisation of subject	2022/2023
Education level	second-cycle studies	Subject group	Optional 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	Polish
Semester of study	1	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Computer Communications -> Faculty of Electronics, Telecommunications and Informatics		
Name and surname of lecturer (lecturers)	Subject supervisor	dr hab. inż. Jerzy Konorski	
	Teachers	dr hab. inż. Jerzy Konorski	

Lesson types and methods of instruction

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	30.0	0.0	0.0	15.0	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	6.0	24.0	75

Subject objectives

The aim of the subject is to present basic knowledge and skills regarding cryptographic mechanisms. During classes students get to know elementary threats and countermeasures, cryptography basics, cryptographic protocols and various asymmetric cryptography implementations and applications such as digital signature, timestamping, PKI. Additionally, subjects directly related to cryptography are also presented, e.g. privacy and anonymity, database security or quantum and post-quantum cryptography elements. Students get to know practical aspects of selected topics during project classes.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[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	During projects students integrate/ implement and present security measures applied to a particular scenario.	[SU1] Assessment of task fulfilment
[K7_U42] can solve engineering and research problems including design, assessment and maintenance of information systems and applications, using experimental methods and management techniques	Student is capable of applying the presented security measures in practice.	[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 knows a set of security measures which cover specified security functions.	[SW3] Assessment of knowledge contained in written work and projects

Subject contents	IT security basics. Authentication methods. Introduction to cryptography. Public key cryptography and PKI. Crypto-services. Cryptographics protocols. Privacy and anonymity. Cryptographic protection of databases. Quantum and post-quantum cryptography elements.
Prerequisites and co-requisites	Basic programming skills

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
Project	50.0%	40.0%
Exam	50.0%	30.0%
Colloquium	50.0%	30.0%

Recommended reading

Basic literature	Classes materials and presentations
Supplementary literature	Schneier B.: Practical Cryptography Bilski T., Pankowski T., Stokłosa J.: Bezpieczeństwo danych w systemach informatycznych (in Polish) Stallings W.: Cryptography and Network Security Gollmann D.: Computer security
eResources addresses	Adresy na platformie eNauczanie:

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