University of Gdańsk

Subject card

Subject name and code	Basics of Cryptography, PG_00179317		
Field of study	Podstawy Kryptografii		
Date of commencement of studies	October 2023	Academic year of realisation of subject	2025/2026
Education level	Bachelor's studies	Subject group	Obligatory subject group in the field of study Optional subject group
Mode of study	full-time studies	Mode of delivery	at the university
Year of study	3	Language of instruction	Polish
Semester of study	5	ECTS credits	2.0
Learning profile	practical	Assessment form	credit
Conducting unit			
Name and surname of lecturer (lecturers)	Subject supervisor	dr Andrzej Borzyszkowski	
	Teachers	dr Andrzej Borzyszkowski	

Lesson types	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	0.0	0.0	30

Subject objectives	Providing knowledge about modern cryptography, learning in practice with some of the most important tools used in modern cryptography.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[INFL3_W02] has ordered, theoretically founded general knowledge in artificial intelligence, formal languages, numerical methods	is able to assess the legality of various activities related to breaking ciphers	[SW4] test/egzamin - ustny lub pisemny [SW2] prezentacja/projekt/referat/ raport
[INFL3_K01] knows the limitations of their own knowledge and understands the need for further education	is aware of the possible threats in the context of using computers and has knowledge about the solutions used, understands how asymmetric cryptography works, what an electronic signature is, what methods are used to check the integrity of documents, understands the possibilities and limitations of modern cryptography, knows basic cryptographic algorithms and protocols, knows possible attacks on the security of information processing systems.	[SK2] prezentacja/projekt/referat/ raport [SK4] test/egzamin - ustny lub pisemny
[INFL3_U01] can apply mathematical knowledge to formulate, analyse and solve tasks related to computer science, design and analyze algorithms in terms of their correctness and computational complexity	is able to create a secure password, generate an X.509 or PGP certificate, compute a hash function, write programs for encryption and cryptanalysis in various cryptographic systems.	[SU2] prezentacja/projekt/referat/ raport [SU4] test/egzamin - ustny lub pisemny

Subject contents

Main concepts and assumptions of cryptography, symmetric and asymmetric cryptography, classical ciphers. The concept of a perfectly secure cipher, one-time pad, random and pseudorandom numbers, stream cipher.
Pseudorandom functions and permutations. Block ciphers and their modes.
Data integrity: MAC and hash functions, properties of hash functions, birthday attack. "Encrypt, then authenticate".
Private key cryptography and public key cryptography. The idea of asymmetric cryptography, attack man-in-the-middle, authentication and signature, hybrid cipher.
Implementation of public key cryptography: Group theory, Fermat's theorems, Euler's theorems. Hard problems: factoring problem, RSA problem, discrete logarithm problem, Diffie-Hellman problem. RSA, ElGamal system.
Digital signature schemes, in symmetric and asymmetric cryptography, RSA, ElGamal and DSS schemes, use of hash functions in signature. Public key infrastructure, X.509, PGP. Certification centers in Poland. PGP in practice.
Elements of steganography.

Prerequisites and co-requisites

Assessment methods and criteria

Subject passing criteria	Passing threshold	Percentage of the final grade
lab	51.0%	70.0%
final test	51.0%	30.0%

Recommended reading

Basic literature	1. J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008. 2. W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall , 2005. 3. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2008
Supplementary literature	none
eResources addresses	

Example issues/ example questions/ tasks being completed	Which of the following block cipher modes allow an attacker to change the order of encrypted blocks without being noticed? (a) ECB (b) CTR (c) CBC (d) OFBModern asymmetric key cryptography is a breakthrough discovery because:(a) it provides radically better efficiency of the encryption(b) it enables communication between participants who have not previously communicated(c) it enables the implementation of the idea of non-repudiation of document authorship(d) it guarantees the authentication of participants
Work placement	Not applicable

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