University of Gdańsk

Subject card

Subject name and code	Introduction to cryptography, PG_00168371		
Field of study	Informatics		
Date of commencement of studies	October 2024	Academic year of realisation of subject	2026/2027
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	Institute of Informatics -> Faculty of Mathematics, Physics and Informatics -> Rector		
Name and surname of lecturer (lecturers)	Subject supervisor	dr Andrzej Borzyszkowski	
	Teachers		

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

To provide knowledge about modern cryptography, to gain practical experience with some of the most important tools used in the field.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[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 the possibilities and limitations of modern cryptography	[SK2] presentation/project/paper/ report [SK4] test/exam - oral or written
[INFL3_W02] has ordered, theoretically founded general knowledge in artificial intelligence, formal languages, numerical methods	understands how asymmetric cryptography works, what an electronic signature is, what methods are used to check the integrity of documents knows basic cryptographic algorithms and protocols, knows possible attacks on the security of information processing systems	[SW4] test/exam - oral or written [SW2] presentation/project/paper/ report
[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] presentation/project/paper/ report [SU4] test/exam - oral or written

Subject contents

- Key concepts and principles 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, the birthday attack. "Encrypt, then authenticate".
- Private key cryptography vs public key cryptography. The concept of asymmetric cryptography, man-in-the-middle attack, authentication and signatures, hybrid ciphers.
- Implementation of public key cryptography: Group theory, Fermat's and Euler's theorems. Hard problems: the factoring problem, the RSA problem, the discrete logarithm problem, the Diffie-Hellman problem. RSA, ElGamal system.
- Digital signature schemes, in symmetric and asymmetric cryptography, RSA, ElGamal and DSS schemes, the use of hash functions in signatures. Public key infrastructure, X.509, PGP. Certification authorities 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%	60.0%
final test	51.0%	40.0%

Recommended reading

Basic literature	lecture materials on the website and the educational portal
Supplementary 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
eResources addresses	

Example issues/ example questions/ tasks being completed

- Which of the following block cipher modes allow an attacker to manipulate the order of the encrypted blocks without being detected? (a) ECB (b) CTR (c) CBC (d) OFB
- Modern asymmetric key cryptography is a breakthrough discovery because: (a) it provides radically better encryption performance (b) it enables communication between participants who have not previously communicated (c) it enables the implementation of the concept of non-repudiation of document authorship (d) it guarantees the authentication of participants
- Which of the following properties do/should hash functions have: (a) uniqueness—no two documents have the same hash (used in digital signatures) (b) weak collision resistance—it is difficult to modify a file while preserving the hash (used in integrity checking) (c) irreversibility – knowing the hash, it is difficult to reconstruct the original data (used in password storage) (d) unpredictability – even a small change results in a large change in the hash

Work placement

Not applicable

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