University of Gdańsk

Subject card

Subject name and code	Security of IT Systems, PG_00203646		
Field of study	Informatics		
Date of commencement of studies	October 2026	Academic year of realisation of subject	2027/2028
Education level	Master's 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	part-time studies	Mode of delivery	at the university
Year of study	2	Language of instruction	Polish
Semester of study	3	ECTS credits	5.0
Learning profile	academic	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	20.0	0.0	20.0	0.0	0.0	40

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	40	0.0	85.0	125

Subject objectives

To provide knowledge about modern cryptography and to gain hands-on experience with some of the most important tools used in this field.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[INFMU2_U11] is able to ensure the availability, reliability and security of IT services, design and apply basic security mechanisms	can create a secure password, generate an X.509 or PGP certificate, compute a hash function, and write programs for encryption and cryptanalysis in various cryptographic systems	[SU2] presentation/project/paper/ report [SU4] test/exam - oral or written
[INFMU2_W06] knows and understands in depth the concepts of functioning of modern IT systems, understands security threats occurring in networked and distributed systems, knows modern models of data processing and storage	understands how asymmetric cryptography works, what an electronic signature is, and what methods are used to verify document integrity; is familiar with basic cryptographic algorithms and protocols; and is aware of potential attacks on the security of information processing systems	[SW4] test/exam - oral or written [SW2] presentation/project/paper/ report

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: MACs and hash functions, properties of hash functions, the birthday attack. “Encrypt, then authenticate.” • Private-key cryptography versus public-key cryptography. The idea of asymmetric cryptography, the man-in-the-middle attack, authentication and digital 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, the ElGamal scheme. • Digital signature schemes in symmetric and asymmetric cryptography; RSA, the ElGamal scheme, and DSS; the use of hashes 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
test	51.0%	40.0%
lab - projects	51.0%	60.0%

Recommended reading	Basic literature	lecture materials on the website and the educational portal
	Supplementary literature	• J. Katz, Y. Lindell, Introduction to modern cryptography, Chapman&Hall/CRC, 2008. • W. Trappe, L. Washington, Introduction to Cryptography with Coding Theory, Prentice Hall , 2005. • 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	• Provide the definition of a perfectly secure cipher. Does such a cipher exist? Why do we use ciphers that are not perfectly secure? • Give examples of nondeterministic ciphers. Is nondeterminism a disadvantage or an advantage of a cipher? Justify. • What new possibilities does asymmetric cryptography offer? What are its limitations? • What properties should a hash function have in cryptography? Explain these properties in the context of hash function applications.	
Work placement	Not applicable	

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