COURSE UNIT DESCRIPTION

Course unit title	Course unit code
Methods of cryptography	

Lecturer(s)	Department where the course unit is delivered
Coordinator: Vilius Stakėnas **Other lecturers:**	Department of Computer Science II Faculty of Mathematics and Informatics Vilnius University

Cycle	Type of the course unit
2nd (MS)	Compulsory

Mode of delivery	Semester or period when the course unit is delivered	Language of instruction
Face-to-face	1 semester	Lithuanian and English

Prerequisites
Basic courses in mathematics, programming skills

Number of ECTS credits allocated	Student's workload	Contact hours	Individual work
5	135	64	71

Purpose of the course unit: programme competences to be developed		
Students will be introduced to the data security problems in computer communication systems and the methods of cryptographic protection, will be able to choose, modify, realize appropriate cryptographic algorithms, will understand their theoretical basis, security issues, will be able to use them in the general data security framework, apply cryptanalysis of partial cases, become familiar with the development of modern cryptography.		
Learning outcomes of the course unit	**Teaching and learning methods**	**Assessment methods**
Students will have the ability to explain the principles of construction of modern symmetric ciphers (block and stream ciphers), will be able to use them, apply cryptanalysis of simple cases, will be acquainted with the encryption algorithms widely used in practice, will be able to use them.	Lectures, demonstrations of computations using computer programs, analysis of examples, regular quizzes, solution of exercises, individual and group consultations. Individual reading.	Review of solutions of assigned exercises, answers to quizzes, final examination in the form of written test.
Students will be introduced to mathematical foundations of public key cryptography, will be able to program the basic computational algorithms and use them in cryptographic schemes.		
Students will have the ability to explain the most important schemes of public key cryptography (encryption and digital signature schemes), will be able to program the algorithms, evaluate the security issues and apply cryptanalysis of simple cases.		
Students will be able to solve the real life problems related to protection the computer communications (authentication, key distribution), perform the cryptographic protocols, will be able to model, analyse and evaluate them.		
Students will be able to demonstrate a detailed knowledge of variety of cryptographic protocols being used for special purposes: secret sharing, commitment, electronic voting,		

digital money, will be able to model and analyse them.		

Course content: breakdown of the topics	Individual work: time and assignments							
	Lectures	Tutorials	Seminars	Laboratory work	Internship/work placement	**Contact hours**	**Individual work**	**Assignments**
1. The aims of cryptographic data protection: confidentiality, authenticity of the data and sources, non-repudiation. Cryptosystem. Security criteria. The algorithms and protocols.	2					**2**	**2**	Individual reading.
2. Symmetric key cryptography. The design principles of the block ciphers: Feistel scheme, substitution-permutation network. The symmetric key encryption standards (DES, AES), other widely used ciphers. Modes of operation. Methods of cryptanalysis. Overview of projects NESSIE, Cryptrec. Construction of the stream ciphers. Stream ciphers used in practice. Methods of cryptanalysis. eStream project.	8			10		**18**	**12**	Cryptanalysis of Vigenere cipher. Decryption of Enigma cipher. Modelling of Feistel scheme, modes of operation. Cryptanalysis of the stream ciphers. Statistical analysis of the pseudorandom streams of bits.. Individual reading.
3. Hash functions. Construction principles. MD, SHA hash functions, Usage of hash functions for data integrity and authentication. Message authentication codes.	4			2		**6**	**6**	Modelling of hash functions, construction of collisions. Individual reading.
4. Key distribution and authentication with symmetric key cryptography. The Wide-Mouth-Frog, Needham-Schroeder, Kerberos protocols. Analysis of attacks.	2			2		**4**	**4**	Modelling of Needham-Schroeder protocol, Merkle puzzles. Individual reading.
5. Mathematical foundations of public key cryptography. Structures and algorithms of number theory: computation with given modulus, Fermat theorem, Chinese remainder theorem, quadratic congruences, discrete logarithms, factorization of integers.	2			2		**4**	**8**	Computational exercises: algorithms of factorization, computing of the discrete logarithms. Individual reading.
6. Public key cryptography: encryption and digital signature schemes. Knapsack, RSA, Rabin, ElGamal cryptosystems, cryptanalysis of special cases. Digital signature schemes: RSA, ElGamal, DSS, Rabin. Security issues.	6			8		**14**	**12**	Decryption and cryptanalysis of knapsack, RSA, Rabin, ElGamal ciphers. Computation of digital signatures. Individual reading.
7. Certification of public keys. X.509 certificate. PGP, SSL, identity based cryptography. Key distribution and authentication protocols with public key cryptography. Diffie-Hellman key distribution protocol.	2			2		**4**	**4**	Public key certification exercise. Individual reading.
8. Secret sharing protocols: Shamir, Asmoth-Bloom secret sharing with thresholds, secret	4			4		**8**	**6**	Exercises for distribution and recovering of the secret. Modelling of zero

sharing for access structures. Applications in encryption and digital signing schemes. Zero knowledge proofs and their applications.								knowledge protocols. Individual reading.
9. Advanced cryptographic protocols: digital money, electronic voting and auctions.	2			2		**4**	**7**	Exercises for modelling digital cash and electronic voting protocols.
10. Preparation for final exam.							**10**	
Total	**32**			**32**		**64**	**71**	

Assessment strategy	**Weight %**	**Deadline**	**Assessment criteria**
Work at the classes, solving homework assignments	40	In the course of semester	Solutions of individualized assignments are required to be submitted until the next laboratory work. Solutions are credited with points. The grade for the laboratory work is computed by the formula 4◈ sum of the points accumulated/maximal number of points.
Quizzes	0-30	In the course of semester	Correct answer to individualized short question at the end of lecture is credited with 0,2 grade. The sum accumulated is included into the final grade.
The final exam	30 -60	Exam session	The weight of the individualized set of questions for the final exam is equal to 50 - sum accumulated for quizzes. The answers are credited with points. The sum obtained with the sum accumulated in the course of semester form the final grade.

Author	**Publishing year**	**Title**	**Issue No or volume**	**Publishing house or Internet site**
Required reading				
D. Stinson	2005	Cryptography Theory and Practice		Taylor & Francis
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone	2001	Handbook of applied cryptography		http://cacr.uwaterloo.ca/hac/
N. Smart	2002	Cryptography, An Introduction : Third Edition		http://www.cs.bris.ac.uk/ ~nigel/Crypto_Book/
Optional reading				
Bruce Schneier	1995	Applied Cryptography: Protocols, Algorithms, and Source Code in C		Wiley