BASIC INFORMATION:

	Code	*Content*
Organizational unit	01.07.300.	College of Information Technologies
Abbreviation	**FIT-CIT**	
Department	01.06.050.	Department of Computer Communications, Networks and Protection
Subject/module	1.02.02.06.003.	**Fundamentals of cryptography**

TYPE OF SUBJECT:

Functional area	**Specialist**
Level of abstraction	**Advanced**
Type of course-obligation	**Mandatory**

COURSE REGISTER:

	Code	*Content*
Scientific area	1	Natural sciences
Scientific field	1.02	Computers and IT
Narrow scientific area	1.02.02.	IT
Scientific sub-area	1.02.02.06.	Other IT areas
Scientific discipline	1.02.02.06.003.	Fundamentals of cryptography

COURSE DESCRIPTION:

Educational and professional goals	The aim of the course is for students to acquire basic knowledge in the field of cryptography, especially in the environment of application of information technology. The goal of scientific study of this course is theoretical and practical. Students should master the basic concepts in the field of cryptography and cryptographic algorithms. Due to the importance of information as the (most important) resource of the business system, the issue of their security and protection through the application of cryptographic methods comes to the fore. In that sense, in order to achieve a high level of security and protection of information, it is necessary to apply appropriate cryptographic methods.
Competences/educational outcomes	The basic course in the fundamentals of cryptography presupposes introduction to the theoretical and practical aspects of cryptography and cryptographic algorithms, regardless of the applied technology, on the one hand, and with the emphasized application of information technology, on the other hand. This course should enable students to acquire basic knowledge that is the basis for the application of cryptographic methods in order to achieve information security.
Mastered skills:	Students are able to understand cryptographic algorithms at a basic level and to perform the duties of a senior cryptography officer in the appropriate public administration services of the police and army, as well as in other positions where knowledge of cryptographic techniques is required.

Course content:	The course is realized through the following contents: Basic concepts from the theory of cryptography. The notion of a system of perfect secrecy. Vernam's code. Shannon's theorem of absolute secrecy. Types of cryptographic algorithms. Symmetric cryptographic algorithms. Sequential symmetric cryptographic algorithms. Self-synchronizing scramblers. Random and pseudorandom array systems. Pseudorandom array generators (GPSN). Basic elements of symmetric cryptographic algorithms. Aspects of secret and commercial cryptography. Examples of commercial sequential symmetric algorithms. Block cipher algorithms. Examples of commercial block cipher algorithms. Multiplicative block codes. The concept of asymmetric cryptographic algorithms. Examples of commercial asymmetric cryptographic algorithms. One-way hash cryptographic algorithms. Examples of commercial hash algorithms. Digital signature. Digital envelope. Aspects of application of cryptographic algorithms. Consideration of cryptographic key lengths and hash values in modern cryptographic algorithms from the population of cryptographic quality. User authentication systems. Basic components of user authentication. Message Authentication Codes (MAC). HMAC algorithms. Dynamic password. HOTP and TOTP algorithms. Challenge-Response systems. OCRA algorithm. TDS (Transaction Data Signature) algorithms. EMV payment systems. CAP/DPA authentication algorithms. New trends in cryptography.

COURSE METRIC: Regular

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
5	**30**	20				85	15	**150**

COURSE METRIC: Extramural

ECTS	Teaching activities (classes)					Individual work		TOTAL working hours
	Contact lessons	Exercise trainings	Seminar and stud. papers	Pedagogical workshops	Prof. and clin. practice	Individual and group study	Research	
5	**15**	20				100	15	**150**

Lecture languages	**Languages of the people of BiH**			

PREREQUISITES FOR ACCESS

Code	Course/module title	Grade	Description of conditions (additional)
1.02.02.03.001.	Information system design		
2.09.08.001.	Network computing		
1.02.01.04.003.	Protection of computer and business systems		
1.02.01.04.005.	Cyber law		

COURSE METHODOLOGY

During the course, the following activities are envisaged

- ☑ 45 contact hours of interactive lectures;
- ☑ 20 hours for exercises in the field of cryptographic protection of computer and business systems;
- ☑ 85 hours of individual learning for full-time students or
- ☑ 100 hours of individual learning for extramural students;
- ☑ 15 hours of research.

Lectures according to the established schedule with the use of modern presentation and demonstration tools and techniques with the application of interactive methods of working with students, which provides insight into their prior knowledge and specific experiences based on the issues, but also insight into the continuity of mastering the material. 45 contact hours of interactive teaching are planned for the subject "Fundamentals of Cryptography".

Lectures are conducted using didactic and educational content in electronic and digital form (which includes recorded lectures and mentoring exercises) on various video presentation media (interactive multimedia optical media).

Application of **information and communication technologies** (ICT) that enable students through Computer Assisted Learning & Research to achieve an active relationship in the process of acquiring knowledge with the help of computer and communication technology, to achieve deeper interaction with teaching content and application of research techniques the very process of acquiring knowledge.

Exercises are intended to acquire practical skills and elaborate practical aspects of various software and hardware technologies for the protection of computer and business systems. The content of the exercises is accompanied by thematic units of lectures. During the exercises, the student is obliged to consult with the heads of the competent Department of Computer Communications, Networks and Protection. As specific forms of exercises, **repeaters** are used where assistants/demonstrators prepare students for the exam by offering them a concise overview of the main points of a particular subject. 20 contact hours of exercises are planned for the subject "Fundamentals of Cryptography".

Exercises will be performed in the computer room of the Pan-European University or in the Laboratory for Information and Communication Technologies and Distance Learning: (ICT-information & communication technologies & DL-distance learning) or. in university laboratories or in authorized laboratories and/or institutions with which the Pan-European University has concluded agreements on teaching-scientific and business-technical cooperation in which the name and status of the partner institution, teaching base, i.e. university clinical center and university laboratory.

In addition to the planned individual and group learning for the planned duration, it is planned that the student will spend 15 hours researching the source.

STUDENT EVALUATION

No.	Evaluation type	Partial/ Final	Optional/ Mandatory	Perc. of part.
01	Exercise	Final	Mandatory	15%
02	Two colloquiums	Partial	,,	30%
03	Seminar paper	Final	,,	15%
04	Final exam	Final	,,	40%
05				

LITERATURE/RESOURCES (listed in order of importance)

Author (name and surname)	Publication title	Publ. seat	Publisher	Issue year	Type of publ.*
a/ Basic literature					
B. Schneier	Applied Cryptography		John Wiley & Sons		coursebook
Charles P. Pfleger	Security in Computing		Prentice Hall		coursebook
Dasgupta**,** Dipankar, Arunava**,** Roy, Nag, Abhijit	Advances in User Authentication		Springer	2017	coursebook
Prof. Dr.Milan Marković	Fundamentals of Cryptography – Lecture materials			2017	script
b/ Additional literature					
Prof. Dr.Milan Marković	Fundamentals of cryptography			2017	presentations

Prof. Dr.Milan Marković	Additional materials on the new trends in cryptography			2017	

c/ Other resources - journals

Author name and surname *(if the resource is an article)*	Journal title	Publ. seat	Publisher	Issue year	Type of journal

d/ Other resources – WEB

Website	Webpage	Paper title/hyperlink	Read

(*)Type of publication (coursebook, script, compendium, multimedia)