UNIVERSITY OF PRIZREN
FACULTY OF COMPUTER SCIENCE

PROGRAM: TIT

Curriculum - – SYLLABUS							
Level of studies	Bachelor	***Program***	TIT	***Academic year***	17/18		
SUBJECT	Cryptography and Authentication						
Year		***Status Of the subject***	Obligatory	***Code***		***ECTS credits***	6
Semester							
Teaching weeks		***Hours teaching***		***Lectures***	***Exercises***		
				30	30		
Teaching Methodology	**Lecturing, lab exercises, projects, individual tasks**						
Consultation							
The teacher	**Fesal Baxhaku**	***E-mail:***	**fbaxhaku@gmail.com**				
		Tel.:	049-254-395				
Assistant		***E-mail:***					
		Tel.:					

Study goal and table of content	Benefits of student
Equiping students with knowledge on how to create secure systems in order to guarantee Information integrity, authenticity and security on the Internet. Also, it includes understanding on how to protect ourselves against possible attacks and how to design and evaluate secure solutions in modern technology.	After attending the course students will: - Understand basic principles of cryptography and general cryptanalysis - Be acquainted with the concepts of symmetric encryption and authentication - As well as public key encryption, digital signatures, and key establishment. - know and understand common examples and uses of cryptographic schemes, including the AES, RSA-OAEP, the Digital Signature Algorithm, and the basic Diffie-Hellman key establishment protocol, and know how and when to apply them. - Be able to compose, build and analyze simple cryptographic solutions.

Methodology for the implementation of educational topics:
Conditions for realization of educational topics:
•

Ways of assessing of the student (in %) :	Evaluation in%	Final grade
Periodic Exam	25%	50 - 59 mark 6 60 – 69 mark 7 70 – 79 mark 8 80 – 89 mark 9 90-100 mark 10
Presentation	10%	
Periodik Exam	25%	
Attendance	5 %	
Final Exam	35 %	

Total	**100.00 %**	

Obligations of student: Attend Lab and Lectures	
Lectures	**Exercises**

Activities	**Hour/ weeks**	**Days/Weeks**	
Lectures	2	14	28
Laboratory exercises	2	14	28
Contacts with teachers / consultations	1	10	10
Practical work	-	-	-
Projects, presentations, etc.	3	12	36
Own study time	2	10	20
Preparation for final exam	3	10	30
Time spent in the assessment (tests, final exam, etc.)			
Notice: 1 ECTS credits= 25 hour commitment, e.g. if the subject has 6 ECTS credits student must have 150 hours during the semester commitment.		**Total load:**	**152**

Week	**Lectures**	**Hour**	**Exercises**	
	Topic		**Topic**	
1.	Introduction to Cryptography and Information Security	2	Lab: Why we need cryptography? Internet demonstration	2
2	Classical encryption techniques	2	Lab: Cesar encoding	2
3.	Classical encryption techniques (2)	2	Lab: Substitution techniques	2
4.	Classical encryption techniques: Enigma and Rotor machines (2)	2	Lab: One-Time Pad, Rail Fence, Rotor machines	
5.	Block Ciphering: DES (Data Encryption Standard)	2	Lab : DES	2
6.	Numbers Theory	2	Lab: Euclidian Algorithm and extended Euclidian Algorithm	
7.	Block Ciphering: AES	2	Lab: AES and keys	2
8.	Intermediary exam	2		
9.	Public Key Cryptography	2	Examples from Number Theory and Chinese remainder theorem	2

10.	RSA Algorithm. How it works?	2	Lab: RSA	2
11	Diffie-Hellman key exchange	2	Lab Diffie Hellman	2
12.	Cryptography with Elliptic Curves	2	Lab: Elliptic Curves	2
13.	Cryptography with Hash-Functions: SHA-1	2	Lab: Hash functions	2
14.	Message Authentication Codes	2	Lab: Message Authentication	2
15.	Work Presentation	2	Work Presentation	2

LITERATURE:

Literature:

1. **William Stallings: Cryptography and Network Security. Principles and Practices (6th Edition). 2016**

2. Ch. Paar, J. Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. 1st edition, Springer, 2009

NOTICE:

Notice for the student: