SYLLABUS

Basic information of the course	
University:	**University "Ukshin Hoti" - Prizren**
Academic unit:	**Faculty of Computer Science**
Study program:	**Information Technologies and Telecommunication**
Course:	**Authentication and Cryptography**
Study level:	**Bachelor**
Course status:	**Mandatory**
Study year:	**2**
Number of hours per week:	**2+2**
Credit value - ECTS:	**6**
Time / location:	**It will be published in the university web site!**
Lecturers:	**Assoc. Prof. Dr. Naim Baftiu** **Ass. Arbër Beshiri, Ph. D. c.**
Contact details:	**naim.baftiu@uni-prizren.com** **arber.beshiri@uni-prizren.com**
Course description:	This course deals with cryptography from both a theoretical and practical perspective. It includes the functionality of cryptography, how security is theoretically analyzed, and how we make it operational in practice. This course includes symmetric encryption, block ciphers, message authentication codes, asymmetric encryption (RSA and discrete-value encryption), AES, DES and digital signatures. It will present basic concepts, definitions and results that are formally related to cryptography and authentication.
Course objectives:	Providing students with the knowledge on how to create secure systems so as to guarantee integrity, authenticity of information and security on the Internet. Also, to understand how to guard against potential attacks and how to design and evaluate secure solutions in modern technology.
Learning outcomes:	After completing this course the students will be able to: - understand the basic principles of

	cryptography and cryptanalysis; - become familiar with the concepts of symmetric encryption and authentication, message encryption using public-key encryption, digital signatures and selecting key; - know and understand the usage of cryptographic schemes, including AES, RSA algorithm, digital signature, Diffie-Hellman key distribution, protocol deployment and understand how and when to implement them; - create, build and analyze simple cryptographic solutions.

Contribution on student load (must correspond with learning outcomes)			
Activity	**Hours**	**Days/week**	**Total/hours**
Lectures	2	15	30
Exercise theoretical/laboratory	2	15	30
Practice work	1	2	2
Contact with lecturer/consultations	1	5	5
Field exercises	1	1	1
Midterms	2	2	4
Laboratory exercises	2	2	4
Individual time spent studying (at the library or home)	3	10	30
Final preparation for the exam	5	6	30
Time spent in evaluation (tests, quiz, final exam)	2	3	6
Projects, presentations, etc.	4	2	8
Total			**150**
Notice: 1 ECTS credits = 25 hours commitment, e.g. if the course has 6 ECTS credits student must have 150 hours during the semester.			

Teaching methods:	The course is a combination of lectures, discussions, numerical and laboratory exercises, while the assignments are presented by the laboratory course lecturers!	
Assessment methods:	- Attendance in lectures and exercises: 5% - Semestral project/lab assignments: 35%. - Midterm 1: 30%. - Midterm 2: 30%. - Or final exam: 100%.	
Assessment and grading:	**Vlerësimi në %**	**Nota përfundimtare**

	91% - 100%	10
	81% - 90%	9
	71% - 80%	8
	61% - 70%	7
	51% - 60%	6
	0% - 50%	5

Literature	
Basic literature:	1. William Stallings. Cryptography and Network Security. Principles and Practices. Pearson. 8th Edition, 2019. N. Deepa. IT Security and Cryptography Lab, 2017.
Additional literature:	1. Christof Paar and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010. 2. Behrouz A. Forouzan. Cryptography and Network Security. McGraw-Hill, 2007.

Study plan	
Week	**Lectures**
First week:	• Introduction to course organization - syllabus (about lectures). • Computer and network security concepts.
Second week:	• Introduction to number theory - Euclidian algorithm.
Third week:	• Symmetric ciphers - classical encryption techniques (1).
Fourth week:	• Classical encryption techniques (2).
Fifth week:	• Block Ciphers and the Data Encryption Standard (DES) - simple DES.
Sixth week:	• Concepts from number theory and finite fields.
Seventh week:	• AES and simple AES (1).
Eighth week:	• First midterm.
Ninth week:	• AES and simple AES (2).
Tenth week:	• Public-key cryptography and RSA
Eleventh week:	• Diffie-Hellman key exchange. • Elgamal cryptographic system. • Elliptic curve arithmetic. • Elliptic curve cryptography.
Twelfth week:	• Hash functions and Secure Hash Algorithm (SHA). • SHA3 and MD5. • Authentication of messages with Hash functions.
Thirteenth week:	• Message authentication codes. • Security of MACs.

	• MACs based on hash functions (HMAC).
Fourteenth week:	• Digital signatures. • Elgamal digital signature scheme. • Elliptic curve digital signature algorithm.
Fifteenth week:	• Second (final) midterm.

Exercises

Study plan	
Java	**Exercises**
First week:	• Introduction to course organization – syllabus (about exercises). • Computer and network security concepts.
Second week:	• Euclidian algorithm. • Cesar cipher - encryption and decryption.
Third week:	• Mono-alphabetic cipher - encryption and decryption. • Transposition cipher (rail fence) - encryption and decryption.
Fourth week:	• Playfair cipher - encryption and decryption. • Hill cipher - encryption and decryption.
Fifth week:	• Vernam cipher - encryption and decryption. • Vernam cipher (One-Time Pad) - encryption and decryption.
Sixth week:	• Vigenere cipher - encryption and decryption. • Steganography.
Seventh week:	• Simple DES - encryption and decryption.
Eighth week:	• Consultations about midterm 1.
Ninth week:	• Extended Euclidean algorithm. • Simple AES - encryption.
Tenth week:	• Simple AES - decryption. • RSA - encryption and decryption.
Eleventh week:	• Diffie-Hellman key exchange.
Twelfth week:	• Hash functions and Secure Hash Algorithm (SHA) • SHA-1 and MD 5.
Thirteenth week:	• Security of MACs. • Digital signature.
Fourteenth week:	• WEP and WPA. • Intrusion Detection System.
Fifteenth week:	• Consultation about midterm 2.

Academic policies and rules of conduct
• Generally lecture presentations will be made through MS PowerPoint, tables, material usage, computer programs and numeric exercises. • Additional resources (scientific papers, publications, national bulletins, as well as recent discoveries and research) will be provided by professors. • In the absence of the opportunity for practical work to be organized weekly, in cooperation with the management of the university, this activity will be organized on certain days in: organizations, companies, etc. • During each session will be organized the conversation and co-participation with the students! • Students are required to be regular in lectures and exercises! • It will be evaluated when the students collaborate and participate in the lectures and course exercises! • Timely arrival in lectures and exercises is mandatory!