Меѓународен Универзитет Визион - International Vision University
Universiteti Ndërkombëtar Vizion - Uluslararası Vizyon Üniversitesi

Adres: Ul. Major C. Filiposki No.1, Gostivar – Makedonya
tel: +389 42 222 325, www.vizyon.edu.mk, info@vizyon.edu.mk

SYLLABUS

COURSE NAME	COURSE CODE	SEMESTER	COURSE LOAD	ECTS
INTRODUCTION TO CRYPTOGRAPHY	**4029**	**5**	**180**	**6**

Prerequisite(s)	None

Course Language	Turkish
Course Type	Elective
Course Level	First Cycle
Course Lecturer	
Course Assistants	
Classroom	
Extra-Curricular Office Hours and Location	**Meeting:** **Consultancy:**

Course Objectives	This course begins with an entry to the subjects of network security and encryption techniques and then goes on by giving information on the design of traditional and modern symmetric encryption algorithms. Also, application areas of these algorithms are identified and a background for symmetric encryption algorithms and cryptographic attacks against these algorithms is provided.
Course Learning Outcomes	• To enable students to learn basic encryption techniques, • To enable students to understand symmetric encryption algorithms and important attacks against these type of algorithms, • To enable students to develope software implementations of a symmetric encryption algorithm with one of the programming languages (for example C).
Course Contents	The course begins with a broad overview of network security topic; we go on to apply some basics of networking. We cover: Introduction to Security Goals, Mathematics of Cryptography, Traditional Symmetric Key Ciphers, Algebraic Structures, Introduction to Modern Symmetric Key Ciphers, Data Encryption Standard, Advanced Encryption Standard, Encipherment Using Modern Symmetric-Key Ciphers, Linear Cryptanalysis, Differential Cryptanalysis, Cryptographic Hash Functions, Symmetric Key Distribution

WEEKLY SUBJECTS AND RELATED PREPARATION STUDIES

Week	Subjects	Related Preparation
1	Introduction to Security Goals	Related Chapters of Course Sources
2	Mathematics of Cryptography	Related Chapters of Course Sources
3	Traditional Symmetric Key Ciphers	Related Chapters of Course Sources
4	Algebraic Structures.	Related Chapters of Course Sources
5	Introduction to Modern Symmetric Key Ciphers	Related Chapters of Course Sources
6	Data Encryption Standard.	Related Chapters of Course Sources
7	Mid-term Exam	Related Chapters of Course Sources
8	Advanced Encryption Standard	Related Chapters of Course Sources
9	Encipherment Using Modern Symmetric-Key Ciphers	Related Chapters of Course Sources
10	Stream Ciphers	Related Chapters of Course Sources
11	Linear Cryptanalysis	Related Chapters of Course Sources
12	Differential Cryptanalysis	Related Chapters of Course Sources
13	Cryptographic Hash Functions	Related Chapters of Course Sources
14	Cryptographic Hash Functions	Related Chapters of Course Sources
15	Final Exam	Related Chapters of Course Sources

ECTS / WORKLOAD TABLE

Presentation / Seminar			
Hours for off-the-classroom study (Pre-study, practice)	14	3	42
Midterm Exam	1	12	12
Final examination	1	14	14
Total Work Load			
ECTS	**6**		

GENERAL PRINCIPLE RELATED WITH COURSE

Dear students,

In order to be included, learn and achieve full success that you deserve in the courses you need to come well prepared by reading the basic and secondary textbooks. We are expecting from you carefully to obey to the course hours, not to interrupt the lessons unless is very indispensable, to be an active participant on the courses, easily to communicate with the other professor and classmates, and to be interactive by participating to the class discussions. In case of unethical behavior both in courses or on exams, will be acting in framework of the relevant regulations. The attendance of the students will be checked in the beginning, in the middle or at the end of the lessons. Throughout the semester the students who attend to all lectures will be given 15 activity-attendance points in addition to their exam grades.

SOURCES

COMPULSORY LITERATURE		
No	**Name of the book**	**Author's Name, Publishing House, Publication Year**
1	Kriptografi / Şifrelerin Matematiği	Canan Çimen , Sedat Akleylek , Ersan Akyıldız ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş., 2007
2	Cryptography and Network Security	Behrouz A. Forouzan
3		

ADDITIONAL LITERATURE		
No	**Name of the book**	**Author's Name, Publishing House, Publication Year**
1	Kriptoloji Uygulamaları	Hüseyin Bodur
2	Introduction to Cryptography with Coding Theory	Wade Trappe and Lawrence C. Washington
3		

EVALUATION SYSTEM

Underlying the Assessment Studies	**NUMBER**	**PERCENTAGE OF GRADE**
Attendance/Participation	15	%10
Project / Event	1	%20
Mid-Term Exam	1	%35
Final Exam	1	%35
TOTAL	**17**	**%100**

ETHICAL CODE OF THE UNIVERSITY

In case of the students are cheating or attempt to cheat on exams, and in the case of not to reference the sources used in seminar studies, assignments, projects and presentations, in accordance to the legislations of the Ministry of Education and Science of Republic of Macedonia and International Vision University, will be applied the relevant disciplinary rules. International Vision University students are expected never to attempt to this kind of behavior.