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

DERS İZLENCESİ (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	

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	1-To enable students to learn basic encryption techniques 2-To enable students to understand symmetric encryption algorithms and important attacks against these type of algorithms. 3-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,

You need to be included in the flow, please follow the course of learning and using that to achieve our success you deserve, you need to practice every day on topics that are covered by the course. It takes practice reading basic and auxiliary literature that is strictly recommended. You should visit classes course I need to make an effort to visit all the professors' lectures. Your activity on the session will be assessed by your professors and the Battle active participant in the discussions that will take place during the time. Students visiting lectures for all at the end if an additional 15 points.

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 GELİŞTİRME VAKFI YAYINCILIK VE İLETİŞİM A.Ş. ,2007
2		
3	Cryptography and Network Security	Behrouz A. Forouzan

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

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 students are cheating on exams or preparation the same, it is not making reference to the source to be used in studies, as for example in assignments, projects and presentation (plagiarism), in accordance with legislations by Ministry of Education and Science of the Republic of Macedonia and İnternational Vision University, apply relevant disciplinary rules. İnternational Vision University students are expected never attempts in this kind of behavior.