

Turkish

T.C. ESKİŞEHİR OSMANGAZİ UNİVERSİTY



Compulsory

FACULTY OF SCIENCES

MATHEMATICS AND COMPUTER SCIENCES DEPARTMENT

COURSE INFORMATION FORM

Course Name					Course Code	
Cryptology						
Number of Course Hours per Week						
Semester	Theory		Practice	- Credit		ECTS
8	3		0	-		4
		C	Course Category (Credi	it)		
Basic Sciences	Engineeri Sciences		Design	General Education		Social
х						
Course Lang	guage		Course Level		Co	ourse Type

Prerequisite(s) if any	
Objectives of the Course	To give basic information about cryptology, to see the place of cryptology in current applications and to see the basic known cryptography algorithms.
Short Course Content	Classical encryption systems: general principles, single-alphabet and multi-alphabet systems, simple analysis methods. General features of public key systems. General features of block and flowing cipher systems. Modern encryption methods. Compression functions and verification codes.

Undergraduate

	Learning Outcomes of the Course	Contributed PO(s)	Teaching Methods *	Measuring Methods **
1	Have a general knowledge of cryptology	2,8	1	А
2	To learn classical cryptography algorithms	8	1	А
3	Learning modern cryptography algorithms	3,8,14	1,2	А
4	To be able to solve examples of encryption and decryption methods	4,8,9	1,2,5	А
5				
6				
7				
8				

^{*}Teaching Methods 1:Expression, 2:Discussion, 3:Experiment, 4:Simulation, 5:Question-Answer, 6:Tutorial, 7:Observation, 8:Case Study, 9:Technical Visit, 10:Trouble/Problem Solving, 11:Induvidual Work, 12:Team/Group Work, 13:Brain Storm, 14:Project Design / Management, 15:Report Preparation and/or Presentation

^{**}Measuring Methods A:Exam, B:Quiz, C:Oral Exam, D:Homework, E:Report, F:Article Examination, G:Presentation, I:Experimental Skill, J:Project Observation, K:Class Attendance; L:Jury Exam

Main Textbook	Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
Supporting References	Neal Koblitz, "A Course in Number Theory and Crytography", Graduate Text in Mathematics, Springer Verlag, 1987. Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, 2002. Johannes Buchmann, "Introduction to Cryptography", Springer-Verlag, New York, 2001. Richard A. Mollin, "RSA and Public-Key Cryptography", Chapman & Hall/CRC, Boca Raton, 2003.
Necessary Course Material	None.

	Course Schedule
1	Introduction
2	Classical encryption
3	Classical encryption
4	Number theory and finite algebras
5	Number theory and finite algebras
6	Block encryption systems
7	Block encryption systems
8	Mid-Term Exam
9	public key systems
10	public key systems
11	Modern encryption
12	RSA
13	El-Gamal
14	AES
15	Digital sign
16,17	Final Exam

Calculation of Course Workload			
Activities	Number	Time (Hour)	Total Workload (Hour)
Course Time (number of course hours per week)	14	3	42
Classroom Studying Time (review, reinforcing, prestudy,)	14	3	42
Homework	5	3	15
Quiz Exam			
Studying for Quiz Exam			
Oral exam			
Studying for Oral Exam			
Report (Preparation and presentation time included)			
Project (Preparation and presentation time included)			
Presentation (Preparation time included)			
Mid-Term Exam	1	2	2
Studying for Mid-Term Exam	1	20	20
Final Exam	1	2	2
Studying for Final Exam	1	30	30
	Toplam iş yükü		
	Toplam iş yükü / 30		
	Dersin AKTS	Kredisi	4

Evaluation				
Activity Type	%			
Mid-term	40			
Quiz	10			
Homework				
Bir öğe seçin.				
Bir öğe seçin.				
Final Exam	50			
Total	100			

Г

NO	PROGRAM OUTCOME			
1	The ability to apply knowledges of Mathematics and Computer Sciences,	4		
2	To have sufficient theoretical and practical knowledge of Mathematics at international level,	5		
3	The ability of describing, modelling and solving of mathematical problems at Mathematics and related subjects,	5		
4	The skill to solve and design a problem process in accordance with a defined target,	5		
5	Skills to analyze data, interpret and apply to other datum and using these data on computer,	4		
6	The skill to use the modern techniques and computational tools needed for mathematical applications,	3		
7	The skill to make team work within the discipline and interdisciplinary,			
8	The ability to improve oneself by following the developments on other modern, scientific and technological subjects as well as Mathematics and Computer Sciences,	4		
9	The skill to communicate orally and in written way, in a clear and concise manner by having individual work skills and ability to independently decide and analytical thinking,	4		
10	The skill to have professional and ethical responsibility,	2		
11	The skill to have consciousness for quality issues and scientific research,	3		
12	The skill to be sensitive to environmental issues related with problems and development of living area and consistent in the social relations,	1		
13	Ability to solve problems in the working life faced to find an appropriate algoritms via mathematical modeling and to write computer programs,	4		
14	The skill to developed design of software systems at different complex levels,	4		
15	The credence of necessity of life-long learning and ability to apply the formation long-life learning.	3		

LECTUTER(S)						
Prepared by	Assoc. Prof. Elis SOYLU YILMAZ					
Signature(s)						

Date:06.06.2024