AYDIN ADNAN MENDERES UNIVERSITY
COURSE INFORMATION FORM

Course Title		Cryptology							
Course Code		MTK560		Couse Level		Second Cycle (Master's Degree)			
ECTS Credit	8	Workload	200 *(Hours)*	Theory	3	Practice	0	Laboratory	0
Objectives of the Course		In this course, the aim is to teach the fundamental subjects and the developments about cryptology. After the students learn the algorithms of cryptology, they will develop some applications using these algorithms.							
Course Content		Introduction to cryptography. History of cryptography. Classical methods of cryptography. Symmetric algorithms. Data encryption standard (DES). Asymmetric algorithms. Rivest, Shamir, Adleman Algorithm (RSA). El Gamal algorithm. Digital Signs Standards. Cryptographic Protocols.							
Work Placement		N/A							
Planned Learning Activities and Teaching Methods				Explanation (Presentation), Discussion, Individual Study					
Name of Lecturer(s)									

Assessment Methods and Criteria

Method	Quantity	Percentage (%)
Midterm Examination	1	30
Final Examination	1	50
Assignment	1	20

Recommended or Required Reading

1	Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1995, ISBN 978-0471117094.
2	Şifreleme Matematiği: Kriptografi (Mathematşcs of Cryptography), Ortadoğu Teknik Üniversitesi, Toplum Bilim Merkezi, Canan Çimen, Sedat Akleylek, Ersan Akyıldız, 2007, ISBN 978-9944-344-27-2.

Week	Weekly Detailed Course Contents	
1	Theoretical	Introduction to cryptography
	Preparation Work	Read the related subjects from the Course Books
2	Theoretical	History of cryptography
	Preparation Work	Read the related subjects from the Course Books
3	Theoretical	Classical methods of cryptography
	Preparation Work	Read the related subjects from the Course Books
4	Theoretical	Classical methods of cryptography
	Preparation Work	Read the related subjects from the Course Books
5	Theoretical	Symmetric algorithms
	Preparation Work	Read the related subjects from the Course Books
6	Theoretical	Symmetric algorithms
	Preparation Work	Read the related subjects from the Course Books
7	Theoretical	Data encryption standard (DES)
	Preparation Work	Read the related subjects from the Course Books
8	Theoretical	Asymmetric algorithms
	Preparation Work	Read the related subjects from the Course Books
9	Theoretical	Asymmetric algorithms
	Preparation Work	Read the related subjects from the Course Books
10	Preparation Work	Read all subjects again
	Intermediate Exam	MIDTERM EXAM
11	Theoretical	Rivest, Shamir, Adleman Algorithm (RSA)
	Preparation Work	Read the related subjects from the Course Books
12	Theoretical	El Gamal algorithm
	Preparation Work	Read the related subjects from the Course Books
13	Theoretical	Digital Signs Standards
	Preparation Work	Read the related subjects from the Course Books

14	Theoretical	Cryptographic Protocols
	Preparation Work	Read the related subjects from the Course Books
15	Theoretical	Cryptographic Protocols
	Preparation Work	Read the related subjects from the Course Books
16	Preparation Work	Read all subjects again
	Final Exam	FINAL EXAM

Workload Calculation

Activity	Quantity	Preparation	Duration	Total Workload
Lecture - Theory	14	3	3	84
Assignment	1	20	2	22
Midterm Examination	1	40	2	42
Final Examination	1	50	2	52
			Total Workload (Hours)	200
			[Total Workload (Hours) / 25*] = **ECTS**	8

**25 hour workload is accepted as 1 ECTS*

Learning Outcomes

1	To be able to comprehend the concepts of cryptology
2	To be able to use the algorithms of cryptology
3	To be able to develop the applications about cryptology using the algorithms
4	To be able to gain the skill of interpreting some interrelations among these concepts
5	To be able to use mathematical concepts in solving certain types of problems

Programme Outcomes *(Mathematics Master)*

1	To be able to have an adequate theoretical and practical domain knowledge.
2	To be able to comprehend the interdisciplinary interaction associated with Mathematics.
3	To be able to use theoretical and practical domain knowledge gained in the field of Mathematics.
4	To be able to interpret knowledge from different disciplines integrating knowledge in the field of mathematics and produce new information.
5	To be able to define, analyse, model and to solve the problems by scientific methods in Mathematics.
6	To be able to conduct a math related specialistic study independently.
7	To be able to develop new strategic approaches to solve problems occurred in unforeseen and complex math-related applications by taking responsibility.
8	To be able to lead in situations that require solving problems related to the mathematics.
9	To be able to criticize his/her knowledge and skills acquired in the field mathematics.
10	To be able to transfer his/her ideas and suggestions for solutions to problems by supporting quantitative or qualitative data verbally and in writing.
11	To be able to communicate both orally and written in a foreign language.
12	To be able to use computer hardware and information technologies with software required by Mathematics.
13	To be able to contribute to the solution of the social, scientific, cultural and ethical problems related to the Mathematics, and being able to support the development of social, scientific, cultural and ethical values.
14	To be able to develop mathematics-related strategies, policies and operational plans, and to evaluate the results obtained within the framework of quality processes.
15	To be able to use his/her knowledge in the field of mathematics and practical problem-solving skills in interdisciplinary studies.

Contribution of Learning Outcomes to Programme Outcomes *1:Very Low, 2:Low, 3:Medium, 4:High, 5:Very High*

	L1	L2	L3	L4	L5
P1	2	3	3	3	3
P2	3	4	4	4	4
P3	4	5	5	5	5
P4	3	4	4	4	4
P12	3	4	4	4	4
P15	4	4	4	4	4