ESOGÜ Mathematics and Computer Sciences Department
COURSE INFORMATION FORM

SEMESTER	Spring

COURSE CODE	821618001	**COURSE NAME**	Cryptology

SEMESTER	**WEEKLY COURSE PERIOD**			**COURSE OF**			
	Theory	**Practice**	**Labratory**	**Credit**	**ECTS**	**TYPE**	**LANGUAGE**
8	3	0	0	3	5	COMPULSORY (x) ELECTIVE ( )	Turkish

COURSE CATAGORY			
Mathematics	**Computer**		**Social Science**
x	x		

ASSESSMENT CRITERIA			
MID-TERM	**Evaluation Type**	**Quantity**	**%**
	1st Mid-Term	1	40
	2nd Mid-Term		
	Quiz		
	Homework		
	Project		
	Report		
	Others (………)		
FINAL EXAM		1	60

PREREQUIEITE(S)	none
COURSE DESCRIPTION	Basic coding systems: general principles, single alphabetic and multi alphabetic systems, simple analysis methods. General features of opening key systems.General information about block and flowing coding systems.General structure of boolean functions, compressing functions and confirming codes.
COURSE OBJECTIVES	Learning general information about cryptology , applications of cryptology to normal life and basic cryptography algoritms.
ADDITIVE OF COURSE TO APPLY PROFESSIONAL EDUATION	Learning applications of cryptology to normal life and training.
COURSE OUTCOMES	Learning general information about cryptology and basic cryptography algoritms.
TEXTBOOK	Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
OTHER 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.
TOOLS AND EQUIPMENTS REQUIRED	None

COURSE SYLLABUS

WEEK	TOPICS
1	General coding systems
2	General coding systems and analysis
3	Number theory and finite objects
4	Opening key systems
5	Opening key systems
6	Boolean functions
7	Boolean functions
8	Midterm
9	Block coding systems
10	Block coding systems
11	Block coding systems
12	Flowing code systems
13	Flowing code systems
14	Compressing functions and confirming codes
15	Compressing functions and confirming codes
16,17	Final Exam

NO	PROGRAM OUTCOMES	3	2	1
1	The ability to apply knowledges of Mathematics and Computer Sciences,	x		
2	To have sufficient theoretical and practical knowledge of Mathematics at international level,	x		
3	The ability of describing, modelling and solving of mathematical problems at Mathematics and related subjects,		x	
4	The skill to solve and design a problem process in accordance with a defined target,		x	
5	Skills to analyze data, interpret and apply to other datum and using these data on computer,	x		
6	The skill to use the modern techniques and computational tools needed for mathematical applications,	x		
7	The skill to make team work within the discipline and interdisciplinary,	x		
8	The ability to improve oneself by following the developments on other modern, scientific and technological subjects as well as Mathematics and Computer Sciences,		x	
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,		x	
10	The skill to have professional and ethical responsibility,		x	
11	The skill to have consciousness for quality issues and scientific research,		x	
12	The skill to be sensitive to environmental issues related with problems and development of living area and consistent in the social relations,		x	
13	Ability to solve problems in the working life faced to find an appropriate algoritms via mathematical modeling and to write computer programs,	x		
14	The skill to developed design of software systems at different complex levels,	x		
15	The credence of necessity of life-long learning and ability to apply the formation long-life learning.		x	
1:None. **2**:Partially contribution. **3**: Completely contribution.				

Instructor(s): Prof. Dr. İ. İlker Akça

Signature: **Date:**