MARMARA UNIVERSITY - FACULTY OF ENGINEERING
2017-2018 Spring
CSE4066 Introduction to Cryptography
COURSE DESCRIPTION FORM

Offering Department	Department of Computer Engineering		Technical Elective
Course Code	CSE4066		
Course Name	Introduction to Cryptography		
Language of Instruction	English		
ECTS	5		
Contact Hours	Theoretical (T): 3	Practice (P):	Laboratory(L):
Pre-requisites	-		
Instructor	**Name**		
	E-mail		
Course Materials	**Mandatory**		
	Recommended	Cryptography: An Introduction, Nigel Smart	
Course Objectives	To learn basic algorithms related to cryptography. To be able to analyze functions and performances of various cryptanalitical and cryptographic algorithms.		
Course Content	Classical cryptographic methods: Classical cryptography, substitution ciphers, mono and poly-alphabetic techniques, etc. Introduction to cryptanalysis. Block ciphers (DES, IDE AES, etc) Public-key Cryptography (modular arithmetic, discrete logarithm, factorization-based methods). Cryptographic protocols (key exchange methods, digital signatures,confidentiality, authentication)		
Learning Outcomes	**LO1**	To define mathematical foundations of cryptography	
	LO2	To describe standard algorithms used in confidentiality, integrity and authentication.	
	LO3	To describe various key sharing and management techniques.	
	LO4	To choose and apply appropriate cryptographic tools for designing a secure system.	
	LO5	To describe basic cryptanalysis techniques.	

Program Outcomes		**LO1**	**LO2**	**LO3**	**LO4**	**LO5**
PO1	Adequate knowledge in mathematics, science (a) and computer engineering subjects (b) pertaining to the relevant discipline (1); ability to use theoretical and applied information in these areas to model and solve engineering problems (2).	1a			1a	
PO2	Ability to identify, formulate, and solve complex engineering problems (a); ability to select and apply proper analysis and modelling methods for this purpose (b).		b	b		
PO4	Ability to devise (a), select, and use (b) modern techniques and tools needed for engineering practice (1); ability to employ information technologies effectively (2).			1b,2	1b	

	No	**Week**	**Subjects**	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**
Subjects (Knowledge, Skills and Behaviours),	**S1**	1-2	Introduction to Cryptography, Classical cryptography techniques	MF				MF
	S2	3-4	Block ciphers, DES, AES		MF		MF, P	MF
Contributions of Subjects to Learning Outcomes,	**S3**	5-6	Number theory, discrete logarithm	MF	MF			
	S4	7	Publick Key Cryptography, RSA		MF		MF, P	
	S5	8	Diffie-Hellman		MF		MF, P	
	S6	9	Ellyptic Curves		MF			
Assessment Methods	**S7**	10	Lattice-based Cryptography		MF			
	S8	11	Hash functions		MF			
	S9	12	Digital Signatures		MF		MF, P	
	S10	13-14	Key exchange and management			MF	MF, P	

	No	**Type**	**Weight**	**Implementation Rule**	**Make-up Rule**
Assessment Methods and Weights	**MF**	Midterm, Final	70%	There will be a midterm and a final exam. Exams will be taken as closed books and lecture notes. Calculater is allowed.	Marmara University regulations will be followed for make-up exams.
	P	Project	30%	A secure and comprehensive system is requested to be designed and implemented using cryptographic tools..	-
	TOTAL		100%		

Determining Letter Grades

- The letter grades will be determined based on the midterm and final exams and quizzes.
- In order to determine the letter grade, a curve or catalog based method will be followed based on the total average scores of the students.
- The final exam score and the total average score of the student must be at least 35 to pass the course.

- According to Marmara University Undergraduate regulations, the weight of the final exam must be at least 40 out of 100.

Assessment	Midterm	Project	Final	TOTAL
Weight	30	30	40	100

Teaching Method, Student Work Load

Time Applied by the Instructor

No	Method	Explanation	Hours
1	Lectures	Lectures are given in class using the board or via presentations. Example questions are solved to enhance the concepts.	14x3=42
2	Problem Session/ Practice	Problems related to the course topics are solved on the board.	
3	Laboratory	Experiments are done in the laboratory or theoretical concepts covered during the lectures are practiced using computer exercises.	
4	Interactive Courses	Questions are asked to students during lectures and they are encouraged to guess the answers (peer learning is also in this category)	
5	Field Work	Students attend activities outside the campus.	
6	Midterm	Midterm exam is given during the midterm week.	2
7	Final	Final exam is given during the final exam week.	2
Estimated Time to be Allocated by a Student			
8	Poject	The students carry out research about the problem given in the project, design and implement their solution and prepare a report.	40
9	Homeworks	The students solve the problems given as homework.	
10	Pre-class learning of Course Material	The students study and learn the new subjects from course materials.	
11	Review of Course Material	Students review the course subjects from course materials to prepare for the exams and homeworks.	35
12	Office Hour	Students ask questions to the instructor or the assistant during office hours.	2
TOTAL			123

Academic Honesty

Violations of scholastic honesty include, but are not limited to cheating, plagiarizing, fabricating information or citations, facilitating acts of dishonesty by others, having unauthorized possession of examinations, submitting work of another person or work previously used without informing the instructor, or tampering with the academic work of other students.

In case academic dishonesty is observed, the first authority is the instructor of the course. The instructor may decide to give the student zero for the homework(s)/lab(s)/exam(s), give the letter grade FF, or may take disciplinary action.