GAU, Faculty of Engineering

Course Unit Title	Introduction to Cryptography
Course Unit Code	CEN479
Type of Course Unit	Technical Elective, engineering students
Level of Course Unit	BSc
National Credits	3
Number of ECTS Credits Allocated	6 ECTS
Theoretical (hour/week)	3
Practice (hour/week)	-
Laboratory (hour/week)	-
Year of Study	4
Semester when the course unit is delivered	7
Course Coordinator	İbrahim Erşan
Name of Lecturer (s)	İbrahim Erşan
Name of Assistant (s)	-
Mode of Delivery	Face to Face, Practical Work, Research
Language of Instruction	English
Prerequisities and co-requisities	-
Recommended Optional Programme Components	Primary computer programming skills

Objectives of the Course

- Conceptual overview of encryption and cryptography standards
- Teaching classical encryption techniques
- Teaching Data Encryption Standart (DES) and Advanced Encryption Standart (AES)
- Application of well known encryption algorithms as practical work

Learning Outcomes		
When this course has been completed the student should be able to		Assesment
1	Have basic skills in encryption techniques and standarts	1
2	Have basic skills in cryptanalysis approaches	1
3	Gain intermediate experience in creating simple ciphering algorithms	3
4	Have knowledge about cryptography techniques depending on DES and AES.	3,4

Assesment Methods: 1. Written Exam, 2. Assignment 3. Project/Report, 4.Presentation, 5 Lab. Work

Course's Contribution to Program

		CL
1	Ability to understand and apply knowledge of mathematics, science, and engineering	3
2	Ability to design and conduct experiments as well as to analyze and interpret data	1
3	Ability to work in multidisciplinary teams while exhibiting professional responsibility and ethical conduct	1
4	Ability to apply systems thinking in problem solving and system design	4
5	Knowledge of contemporary issues while continuing to engage in lifelong learning	
6	Ability to use the techniques, skills and modern engineering tools necessary for engineering practice	2
7	Ability to express their ideas and findings, in written and oral form	4
8	Ability to design and integrate systems, components or processes to meet desired needs within realistic constraints	1
9	Ability to approach engineering problems and effects of their possible solutions within a well structured, ethically responsible and professional manner	1
10	To apply fundamental concepts of software design, database design, data processing and artificial intelligence in the modeling, designing, implementing, testing and deploying software solutions.	4
11	Ability to analyse and design hardware systems by applying the principles of embedded systems, microprocessors, computer networks, distributed systems and data communication.	2

CL (Contribution Level): 1.Very Low, 2.Low, 3.Moderate, 4.High, 5.Very High

Course Contents

Week			Exams
1		Introduction	
2		Characterization of Cryptographic Systems	
3		Classical Encryption Techniques: Caesar Cipher and Playfair Cipher	
4		Classical Encryption Techniques: Hill Cipher & Vigenere Cipher	
5		Classical Encryption Techniques: Steganography & Rotor Machines	
6		Details of Frequancy Analysis, Distribution of Research Topics	
7		Simplified Data Encrytion Standart	Quiz
8			Midterm
9		Fiestel Algorithm and Classification of Cryptology Techniques	
10		Data Encryption Standart, Discussion on Research Topics	
11		Block Cipher Design Principles	
12		Finite Fields, Euclid Algorithm and Polynomials	
13		RSA and Structure of AES	Quiz
14		Presentation of Research Topics	
15			Final

Recommended Sources

Textbook: Cryptography and Network Security – Principles and Practice, W.Stallings, Prentice Hall, Second Edition, 1998

Supplementary Material (s): Handbook of Applied Cryptography, A.J.Menezes, P.C.vanOorschot, S.A.Vanstone, CRC Press, 5th Edition, 2001

Assessment

Attendance	5%	
Homeworks	10%	
Presentation	15%	
Midterm Exam	30%	Written Exam
Quiz	5%	Written Exam
Final Exam	35%	Written Exam
Total	100%	

ECTS Allocated Based on the Student Workload

Activities	Number	Duration (hour)	Total Workload(hour)
Course duration in class (including the Exam week)	13	3	39
Labs and Tutorials	-	-	-
Assignments	4	5	20
E-Learning Activities	-	-	-
Project/Presentation/Report Writing	1	25	25
Quizzes	2	6	12
Lab Exams	-	-	-
Midterm Examination	1	15	15
Final Examination	1	15	15
Self Study	13	3	39
Total Workload			165
Total Workload/30 (h)			5.5
ECTS Credit of the Course			6