Course Description

Course Code	YS 421
Course Name	INFORMATION SECURITY
Prerequisite Courses	
Language of the Course	The English
Course Coordinator	
Instructor(s)	
Course Assistants	
The aim of the course	The aim of this course is to examine the basic mathematical concepts and methods for the analysis, design and simulation of cryptographic algorithms which are developed to provide or improve the security of any information stored in electronic media.
Course Content	Giving basic information about design principles and methods of information encryption and decryption algorithms

Weekly Course Content

Week 1	The importance and historical development of encryption algorithms and basic concepts of data encryption.
Week 2	Investigation of basic principles and classification of classical encryption algorithms
Week 3	Symmetric key-based classical encryption algorithms
Week 4	Symmetric key-based classical encryption algorithms
Week 5	Symmetric key-based classical encryption algorithms
Week 6	Asymmetric key based classical encryption algorithms
Week 7	Asymmetric key based classical encryption algorithms
Week 8	Midterm exam.
Week 9	Hash functions
Week 10	Random number generators
Week 11	Random number generators
Week12	Digital signature
Week 13	Modern encryption algorithms
Week 14	Modern encryption algorithms
Week 15	Final exam.

Course Learning Outcomes

1	Ability to apply math, science and engineering knowledge
2	Ability to analyze and interpret the security risks associated with the use of current technologies
3	-
4	-
5	-
6	-

Contribution of the Course to Program Qualifications

	Contribution of the Course to Program Qualifications	Contribution Level
01	The student will have the ability to apply analytical approach, mathematics and science knowledge in software and engineering issues.	0
02	The student will have the ability to identify, define, formulate and solve a problem in software and computer systems.	0
03	The student will have gains scientific research skills in software and engineering problems, has the ability to design a system, part or process.	0
04	The student will have the ability to use the design capability, techniques and tools required for engineering applications.	0
05	The student will have the ability to design, implement and interpret experimental work and software projects by analyzing the results.	0
06	The student will have the ability to work between disciplines and teamwork.	5
07	The student will have the ability to work in international environments and adapt to different cultures.	0
08	The student will have verbal and written communication skills in Turkish and English.	0
09	The student will have the awareness of the necessity of lifelong learning and the ability to realize it.	0
10	The student will gain knowledge of legal issues with the awareness of professional and ethical responsibility.	0
11	The student will have managerial skills (leadership, organization, time and risk management, quality awareness, efficiency, etc.).	5
12	The student will have the ability to participate in social activities, to acquire regular sports habits and to use time in the best way.	5
13	The student will have the ability to find unusual ways and produce projects.	0
14	The student will have professional self-confidence, being an entrepreneur and taking initiative.	0
15	It is sensitive about the problems of the age and looks after the national interests.	0

ECTS WORKLOAD

	Number	Duration (hours)	Number*Duration
Face to face education	14	2	28
Out-of-class study time (pre-study, reinforcement)	14	1	14
Homeworks	2	4	8
Presentation / Seminar preparation	0	0	0
Quizzes	0	0	0
Preparation for midterm exams	1	8	8
midterm exams	1	2	2
Project (Semester assignment)	0	0	0
Lab	0	0	0
field work	0	0	0
Preparation for the final exam	1	10	10
Semester final exam	1	2	2
Research	4	2	8
TOTAL WORKLOAD			**80**
ECTS			**3**

Evaluation

SEMESTER EVALUATION	Number	Contribution Percentage
Midterm	1	60
Quiz	0	0
Homework	2	40
SEMESTER TOTAL		**100**
Contribution rate of mid-term evaluations to success		40
Contribution rate of the final exam to success		60
GRAND TOTAL		**100**

RESOURCES	
Textbook	Applied Cryptography, Bruce SCHNEIER, John Wiley &Sons, Inc. 1998
Helpful Resources	Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, CRC Press, 2001