ÇANKAYA UNIVERSITY
Faculty of Arts and Sciences
Course Definition Form

Part I. Basic Course Information

Department Name	MATHEMATICS					**Dept. Numeric Code**	27
Course Code	MATH427	**Number of Weekly Lecture Hours**	3	**Number of Weekly Lab/Tutorial Hours**	0	**Number of Credit Hours**	3
Course Web Site	http:// math427.cankaya.edu.tr					**ECTS Credit**	05

Course Name *This information will appear in the printed catalogs and on the web online catalog.*	
English Name	Introduction to Cryptography
Turkish Name	Kriptografiye Giriş

Course Description
Provide a brief overview of what is covered during the semester. This information will appear in the printed catalogs and on the web online catalog. Maximum 60 words.

History and overview of cryptography, The Basic Principles of Modern Cryptography, Private-Key Cryptography; One time pad and stream ciphers, Block ciphers, PRPs and PRFs, Attacks on block ciphers. Message Integrity; Collision resistant hashing, Authenticated encryption: security against active attacks. Public-Key Cryptography; Cryptography using arithmetic modulo primes, Public key encryption, Arithmetic modulo composites. Digital Signatures.

Prerequisites (if any) *Give course codes and check all that are applicable.*	1st	2nd	3rd	4th
	☐ Consent of the Instructor	☐ Senior Standing	☐ Give others, if any.	
Co-requisites (if any)	1st	2nd	3rd	4th
Course Type *Check all that are applicable*	☐ Must course for dept.	☐ Must course for other dept.(s)	☒ Elective course for dept.	☒ Elective course for other dept.(s)

Course Classification
Give the appropriate percentage for each category.

Category	Mathematics & Natural Sciences	Engineering & Architectural Sciences			
Percentage	80	20			

Part II. Detailed Course Information

Course Objectives
Maximum 100 words.

Familiarity with the major algorithms of historical and modern cryptography as documented in open literature; knowledge of issues involved in choice of algorithm and key size; ability to analyze performance of various cryptographic and cryptanalytic algorithms

Learning Outcomes
Explain the learning outcomes of the course. Maximum 10 items.

1. The students will learn concepts related to cryptography including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography and digital signatures.
2. The students will learn basic forms of attack on a crypto system

Textbook(s)
List the textbook(s), if any, and other related main course material.

Author(s)	Title	Publisher	Publication Year	ISBN
Jonathan Katz & Yehuda Lindell	Introduction to Modern Cryptography 2nd edition	Chapman and Hall/CRC	2014	978-1466570269

Reference Books
List, if any, other reference books to be used as supplementary material.

Author(s)	Title	Publisher	Publication Year	ISBN
Douglas R. Stinson	Cryptography: Theory and Practice 2nd edition	Chapman and Hall/CRC	2002	978-1584882060

Teaching Policy
Explain how you will organize the course (lectures, laboratories, tutorials, studio work, seminars, etc.)

3 hours of lecturing per week. Attendance to the lectures is compulsory.

Laboratory/Studio Work
Give the number of laboratory/studio hours required per week, if any, to do supervised laboratory/studio work and list the names of the laboratories/studios in which these sessions will be conducted.

Computer Usage
Briefly describe the computer usage and the hardware/software requirements for the course.

Course Outline
List the weekly topics to be covered.

Week	Topic(s)
1	History and overview of cryptography. The Basic Principles of Modern Cryptography.
2	Private-Key Cryptography; One time pad and stream ciphers.
3	Block ciphers.
4	PRPs and PRFs.
5	Attacks on block ciphers.
6	Message integrity: definition and applications.
7	Collision resistant hashing.
8	Authenticated encryption: security against active attacks.
9	Arithmetic modulo primes
10	Public-Key Cryptography; Cryptography using arithmetic modulo primes.
11	Public key encryption.
12	Arithmetic modulo composites.
13	Digital Signatures: definitions and applications
14	More signature schemes

Grading Policy
List the assessment tools and their percentages that may give an idea about their relative importance to the end-of-semester grade.

Assessment Tool	Quantity	Percentage	Assessment Tool	Quantity	Percentage	Assessment Tool	Quantity	Percentage
Homework	5	20	Case Study			Attendance		
Quiz(es)			Lab Work			Field Study		
Midterm Exam	2	40	Classroom Participation			Project		
Term Paper			Oral Presentation			Final Exam	1	40

ECTS Workload
List all the activities considered under the ECTS.

Activity	Quantity	Duration (hours)	Total Workload (hours)
Attending Lectures (*weekly basis*)	14	3	42
Attending Labs/Recitations (*weekly basis*)			
Compilation and finalization of course/lecture notes (*weekly basis*)	14	1	14
Collection and selection of relevant material (*once*)	1	5	5
Self study of relevant material (*weekly basis*)	14	1	14
Take-home assignments	5	3	15
Preparation for quizzes			
Preparation for mid-term exams (*including the duration of the exams*)	2	10	20
Preparation of term paper/case-study report (*including oral presentation*)			
Preparation of term project/field study report (*including oral presentation*)			
Preparation for final exam (*including the duration of the exam*)	1	15	15
		TOTAL WORKLOAD / 25	125/25
		ECTS Credit	**5**

Total Workloads are calculated automatically by formulas. To update all the formulas in the document first press CTRL+A and then press F9.

Program Qualifications vs. Learning Outcomes *Consider the program qualifications given below as determined in terms of learning outcomes and acquisition of capabilities for all the courses in the curriculum. Look at the learning outcomes of this course given above. Relate these two using the Likert Scale by marking with X in one of the five choices at the right.*

No	Program Qualifications	Contribution				
		0	1	2	3	4
1	Adequate knowledge in mathematics; ability to use applied and theoretical information in these areas to solve pure and applied mathematical problems.				X	
2	Ability to use modern computational tools to analyze an abstract or real life problem					X
3	Adequate knowledge in theoretical and historical background in mathematics				X	
4	Ability to work individually and in teams efficiently, ability to collaborate effectively in teams to analyze complex systems from intra-disciplinary and multi-disciplinary areas				X	
5	Ability to communicate effectively in English about technical subjects, both orally and in writing				X	
6	Ability to use, develop and implement new experiments and algorithms to solve scientific, engineering and financial problems				X	
7	Ability to analyze a mathematical problem using both analytical and numerical methods; use and compare theoretical and simulational methods to gain deeper insight				X	
8	Ability to report the findings, conclusions and interpretations related to a project in the area of pure and applied mathematics, ability to write technical reports, to prepare and conduct effective presentations				X	
9	Recognition of the need for lifelong learning; ability to access information, to follow developments in science and technology, and to keep continuous self improvement				X	
10	Awareness of professional and ethical responsibility issues and their legal consequences					X

Scale for contribution to a qualification: **0**-none, **1**-little, **2**-moderate, **3**-considerable, **4**-highest