TED UNIVERSITY, COURSE SYLLABUS

Faculty	Engineering	**Department**	Computer Engineering

Course Code & Number	CS 525	**Course Title**	Advanced Information Security and Cryptography
Type of Course	☐ Compulsory ☑ Elective	**Semester**	☑Fall ☐ Spring ☐ Summer
Course Credit Hours	(3+0+0) 3	**Number of ECTS Credits**	7.5
Pre-requisite	None	**Co-requisite**	
Mode of Delivery	☑ Face-to-face ☐ Distance learning	**Language of Instruction**	☑ English ☐ Turkish
Course Coordinator	Dr. Elif KURTARAN ÖZBUDAK	**Course Lecturer(s)**	Dr. Elif KURTARAN ÖZBUDAK
Required Reading	Understanding Cryptography:A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl	**Recommended Reading**	- Cryptography and Network Security, 7th Ed., William Stallings - Cryptography: Theory and Practice. 4th Ed., Douglas R. Stinson.

Course Catalog Description	Security concepts with new applications, review of stream ciphers and block ciphers, modern crypto schemes; the Advanced Encryption Standard (AES) in detail, attacks on block ciphers, public key schemes, public key infrastructure, RSA, ECC (Elliptic Curve Cryptography), Diffie-Hellman key exchange, Digital Signature Algorithms, SHA hash function family, authentication. Further topics may be covered such as internet of things, lightweight ciphers for RFIDs, side channel attacks, homomorphic encryption, blockchain, software security and mobile devices.
Course Objectives	This course is intended to review the fundamentals concepts of cryptography and and modern private/public-key cryptographic systems/protocols. The course serves as an introduction for graduate students who are interested in pursuing research and expertise in information security and cryptography.
Course Learning Outcomes	Upon successful completion of this course, a student will be able to 1. Identify basics of cryptographic algorithms being used in information security. 2. Understand block ciphers and stream ciphers 3. Learn how to encrypt information using symmetric and asymmetric encryption algorithms. 4. Learn cryptographic primitives to provide integrity, availability and confidentiality. 5. Be able to combine basic knowledge with applicable methodologies to solve information security related engineering problems.

Learning Activities & Teaching Methods[1]	☒ Brainstorming ☒ Case Study/Scenario Analysis ☐ Collaborating ☒ Concept Mapping ☒ Demonstrating ☒ Discussions / Debates ☐ Drama / Role Playing ☐ Experiments ☐ Field Trips ☒ Guest Speakers	☒ Hands-on Activities ☐ Inquiry ☐ Microteaching ☒ Oral Presentations / Reports ☐ Peer Teaching ☒ Predict-Observe-Explain ☒ Problem Solving ☒ Questioning ☒ Reading	☐ Scaffolding / Coaching ☒ Seminars ☐ Service Learning ☐ Simulations & Games ☒ Telling / Explaining ☐ Think-Pair-Share ☒ Video Presentations ☐ Web Searching ☐ Other(s):……………

Assessment Methods & Criteria[2]	☐ Case Studies / Homework	(…%)	☒ Presentation (Oral, Poster, Report)	(15%)
	☐ Lab Assignment	(...%)	☐ Project	(..%)
	☐ Observation	(...%)	☐ Quiz	(15 %)
	☐ Oral Questioning	(...%)	☐ Self-evaluation	(...%)
	☐ Peer Evaluation	(...%)	☒ Test/Exam	(70%)
	☐ Performance Project (Written, Oral)	(...%)	☐ Other(s):………	(%)
	☐ Portfolio	(...%)		

Student Workload[3]	☐ Case Study Analysis	(... hrs)	☐ Online Discussion	(... hrs)
	☒ Course Readings	(48 hrs)	☒Oral Presentation	(10 hrs)
	☐ Debate	(... hrs)	☐ Poster Presentation	(... hrs)
	☐ Demonstration	(... hrs)	☒ Report on a Topic	(20 hrs)
	☒ Exams/Quizzes	(10 hrs)	☒ Research Review	(20 hrs)
	☐ Field Trips/Visits	(... hrs)	☒ Resource Review	(20 hrs)
	☐ Hands-on Work	(…hrs)	☐ Team Meetings	(... hrs)
	☐ Lab Applications	(... hrs)	☐ Web Designs	(... hrs)
	☒ Lectures	(42 hrs)	☐ Work Placement	(... hrs)
	☐ Mock Designs	(... hrs)	☐ Workshop	(... hrs)
	☐ Observation	(... hrs)	☒ Other(s): Project	(10 hrs)
			Total Workload[4]	180

[1] Multiple options possible.

[2] Multiple options possible. A percentage must be stated for the selected assessment method & criteria.

[3] Multiple options possible. The student workload is found by multiplying the number and duration (hour) of the activity involved.

[4] Computing the ECTS credits of a course: Total workload / 25 or 30 hours = ECTS credit and1 ECTS credit = 25-30 hours

GRADING

A. Midterm [30%]

One midterm exam that is worth 30% of the overall course grade.

B. Quiz [15%]

You will have 2 announced quizzes.

B. Report On a Topic and Presentation [%15]

Each student will learn and analyze one hot-topic in Information Security and Cryptography (such as internet of things, lightweight ciphers for RFIDs, side channel attacks, homomorphic encryption, blockchain, software security and mobile devices) and make a presentation.

C. Final Exam [40%]

One Final exam that is worth 40% of the overall course grade.

COURSE POLICIES

Attendance

Attending is not mandatory but recommended.

Missed Work

Make-up exam will be done **only** for midterm and final exam, if the student can provide a legal document confirming a life threatening health issue at the time of the exam, or with the consensus of the CMPE faculty. (Only one Make up exam will be done at the end of the semester covering both midterm and final). There will be **no make-up for quizzes**.

Late Assignment Submission Policy

Late submissions will be graded with 20% penalty for each day.

Extra Credit

Extra credits will not be offered.

Assignment Rules

All assignment works must be done individually. A student can submit only one work. In case of multiple submissions, only the latest submission will be considered. Students cannot submit work on other students' behalf.

Plagiarism

All of the following are considered plagiarism:

- turning in someone else's work as your own
- copying words or ideas from someone else without giving credit
- failing to put a quotation in quotation marks
- giving incorrect information about the source of a quotation
- changing words but copying the sentence structure of a source without giving credit
- copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not" (www.plagiarism.org)

Plagiarism is a very serious offense and will be penalized accordingly by the university disciplinary committee. The best way to avoid accidentally plagiarizing is to work on your own before you ask for the help of other resources.

Cheating

Cheating has a very broad description which can be summarized as “acting dishonestly”. Some of the things that can be considered as cheating are the following:

- Copying answers on examinations, homework and laboratory works,
- Using prohibited material on examinations,
- Lying to gain any type of advantage in class
- Providing false, modified or forged data in a report
- Plagiarizing.
- Modifying graded material to be regraded.
- Causing harm to colleagues by distributing false information about an examination, homework or laboratory

Cheating is a very serious offense and will be penalized accordingly by the university disciplinary committee.

Class Readings

Class readings are necessary but not mandatory. The material covered in class by your instructor will only provide a fundamental understanding of the general context.

TENTATİVE COURSE OUTLINE

Week	Topics	Readings	Assignments, quizzes, and exams
1 2-6 October	Introduction to Cryptography	Chapter 1.1, 1.2, 1.3	
2 9-13 October	Modular Arithmetic and Historical Ciphers	Chapter 1.4	
3 16-20 October	Stream Ciphers and Random Numbers	Chapter 2.1, 2.2.2.1, 2.2.2, 2.3	
4 23-27 October	Block Ciphers and DES	Chapter 3.1, 3.2, 3.3, 3.4, 3.5	
5 30 Oct.-3 November	Advanced Encryption Standard	Chapter 4.1, 4.2, 4.3, 4.4	Topic Report- First Draft
6 6-10 November	Block Cipher Operations	Chapter 5.1.1, 5.1.2, 5.1.3	Quiz1
7 13-17 November	Introduction to Public-Key Cryptography	Chapter 6.1, 6.2	
8 20-24 November	No Lecture		Midterm

9 27 Nov.-1 December	Number Theory for Public-Key Cryptography	Chapter 6.3	
10 4-8 December	RSA Cryptosystem	Chapter 7.1, 7.2, 7.3, 7.4	
11 11-15 December	Diffie- Hellman Key Exchange and Discrete Log Problem	Chapter 8.1, 8.3, 8.4	
12 18-22 December	Digital Signatures	Chapter 10.1, 10.2	Topic Report- Final
13 25-29 December	Hash Functions	Chapter 11.2, 11.2, 11.4	Quiz 2
14 02-05 January 2024	Message Authentication Codes	Chapter 12.1, 12.2	Presentation

Prepared By & Date	Dr. Elif KURTARAN ÖZBUDAK 25/09/2023	**Revision Date**	

(*) The lectures will be conducted in CMPE-325 course.