

# TED UNIVERSITY, COURSE SYLLABUS

<b>Faculty</b>	Engineering	<b>Department</b>	Software/Computer Engineering
----------------	-------------	-------------------	-------------------------------

<b>Course Code &amp; Number</b>	CMPE 325-N	<b>Course Title</b>	Information Security and Cryptography
<b>Type of Course</b>	<input type="checkbox"/> Compulsory <input checked="" type="checkbox"/> Elective	<b>Semester</b>	2024-2025 <input checked="" type="checkbox"/> Fall <input type="checkbox"/> Spring
<b>Course Credit Hours</b>	(3+0+0) 3	<b>Number of ECTS Credits</b>	5
<b>Pre-requisite</b>	CMPE 211 OR CMPE 114	<b>Co-requisite</b>	
<b>Mode of Delivery</b>	<input checked="" type="checkbox"/> Face-to-face <input type="checkbox"/> Distance learning	<b>Language of Instruction</b>	<input checked="" type="checkbox"/> English <input type="checkbox"/> Turkish
<b>Course Coordinator</b>	Dr. Elif KURTARAN ÖZBUDAK	<b>Course Lecturer(s)</b>	Dr. Elif KURTARAN ÖZBUDAK
<b>Required Reading</b>	Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar, Jan Pelzl	<b>Recommended Reading</b>	- Cryptography and Network Security, 7th Ed., William Stallings  - Cryptography: Theory and Practice. 4th Ed., Douglas R. Stinson.

<b>Course Catalog Description</b>	Security concepts, stream ciphers and random numbers, block ciphers and block cipher operations, modern crypto schemes; the Advanced Encryption Standard (AES), DES, RSA, Diffie-Hellman key exchange, Digital Signature Algorithms, Cryptographic Hash functions, Message Authentication Code, Protocols and key establishment methods, public-key infrastructure.
<b>Course Objectives</b>	The objective of this course is to provide the students the necessary knowledge about the basics of cryptographic algorithms, and utilize these algorithms in computing systems. Describe the use of cryptographic primitives to create secure systems, define and correctly implement cryptographic algorithms for the protection of information at rest and in transit. The students will be able to encrypt the information using symmetric and asymmetric encryption algorithms.
<b>Course Learning Outcomes</b>	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.

--	--

<b>Learning Activities &amp; Teaching Methods<sup>1</sup></b>	<input checked="" type="checkbox"/> Brainstorming <input checked="" type="checkbox"/> Case Study/Scenario Analysis <input type="checkbox"/> Collaborating <input checked="" type="checkbox"/> Concept Mapping <input checked="" type="checkbox"/> Demonstrating <input checked="" type="checkbox"/> Discussions / Debates <input type="checkbox"/> Drama / Role Playing <input type="checkbox"/> Experiments <input type="checkbox"/> Field Trips <input type="checkbox"/> Guest Speakers	<input checked="" type="checkbox"/> Hands-on Activities <input type="checkbox"/> Inquiry <input type="checkbox"/> Microteaching <input checked="" type="checkbox"/> Oral Presentations / Reports <input type="checkbox"/> Peer Teaching <input checked="" type="checkbox"/> Predict-Observe-Explain <input checked="" type="checkbox"/> Problem Solving <input checked="" type="checkbox"/> Questioning <input checked="" type="checkbox"/> Reading	<input type="checkbox"/> Scaffolding / Coaching <input checked="" type="checkbox"/> Seminars <input type="checkbox"/> Service Learning <input type="checkbox"/> Simulations & Games <input checked="" type="checkbox"/> Telling / Explaining <input type="checkbox"/> Think-Pair-Share <input checked="" type="checkbox"/> Video Presentations <input type="checkbox"/> Web Searching <input type="checkbox"/> Other(s):.....
---	--	---	---

<b>Assessment Methods &amp; Criteria<sup>2</sup></b>	<input checked="" type="checkbox"/> Case Studies / Homework	(10%)	<input type="checkbox"/> Presentation (Oral, Poster)	(... %)
	<input type="checkbox"/> Lab Assignment	(...%)	<input type="checkbox"/> Project	(... %)
	<input type="checkbox"/> Observation	(...%)	<input checked="" type="checkbox"/> Quiz	(15 %)
	<input type="checkbox"/> Oral Questioning	(...%)	<input type="checkbox"/> Self-evaluation	(...%)
	<input type="checkbox"/> Peer Evaluation	(...%)	<input checked="" type="checkbox"/> Test/Exam	(70 %)
	<input type="checkbox"/> Performance Project (Written, Oral)	(...%)	<input checked="" type="checkbox"/> Other(s):In class activities	(5%)
	<input type="checkbox"/> Portfolio	(...%)		

<b>Student Workload<sup>3</sup></b>	<input checked="" type="checkbox"/> Case Study Analysis	(15 hrs)	<input type="checkbox"/> Online Discussion	(... hrs)
	<input checked="" type="checkbox"/> Course Readings	(35 hrs)	<input type="checkbox"/> Oral Presentation	(... hrs)
	<input type="checkbox"/> Debate	(... hrs)	<input type="checkbox"/> Poster Presentation	(... hrs)
	<input type="checkbox"/> Demonstration	(... hrs)	<input type="checkbox"/> Report on a Topic	(... hrs)
	<input checked="" type="checkbox"/> Exams/Quizzes	(30 hrs)	<input checked="" type="checkbox"/> Research Review	(10 hrs)
	<input type="checkbox"/> Field Trips/Visits	( hrs)	<input type="checkbox"/> Resource Review	(... hrs)
	<input checked="" type="checkbox"/> Hands-on Work	(20 hrs)	<input type="checkbox"/> Team Meetings	(... hrs)
	<input type="checkbox"/> Lab Applications	(... hrs)	<input type="checkbox"/> Web Designs	(... hrs)
	<input checked="" type="checkbox"/> Lectures	(42 hrs)	<input type="checkbox"/> Work Placement	(... hrs)
	<input type="checkbox"/> Mock Designs	(... hrs)	<input type="checkbox"/> Workshop	(... hrs)
	<input type="checkbox"/> Observation	(... hrs)	<input type="checkbox"/> Other(s):.....	(... hrs)
<b>Total Workload<sup>4</sup></b>			152	

<sup>1</sup> Multiple options possible.

<sup>2</sup> Multiple options possible. A percentage must be stated for the selected assessment method & criteria.

<sup>3</sup> Multiple options possible. The student workload is found by multiplying the number and duration (hour) of the activity involved.

<sup>4</sup> Computing the ECTS credits of a course: Total workload / 25 or 30 hours = ECTS credit and 1 ECTS credit = 25-30 hours

<b>GRADING</b>
<b>A. Midterm [30%]</b>
One midterm exam that is worth 30% of the overall course grade.
<b>B. Quiz [15%]</b>
You will have 2 announced quizzes.
<b>C. Assignments [10%]</b>
You will be given 2 assignments each worth 5%.
<b>D. Active Class Participation [5%]</b>
It is encouraged that you participate in class activities and discussions. Class participation is awarded based on your attendance to written class activities , pop quiz(es) and your contribution to class discussion.
<b>E. Final Exam [40%]</b>
One Final exam that is worth 40% of the overall course grade.
<b>COURSE POLICIES</b>
<b>Attendance</b>
Attending is <b>NOT mandatory</b> , but <b>strongly recommended</b> . Some hands-on activities and discussions will be done in the lectures. If you would like to collect points for these activities ( see active class participation clause), you need to attend the lectures.
<b>Missed Work</b>
Make-up exam will be done <b>only</b> 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 <b>no make-up for quizzes</b> .
<b>Late Assignment Submission Policy</b>
Late submissions will be graded with 20% penalty for each day.
<b>Extra Credit</b>
Extra credits will not be offered.
<b>Assignment Rules</b>
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.
<b>Plagiarism</b>
All of the following are considered plagiarism: <ul style="list-style-type: none"> <li>• turning in someone else's work as your own</li> <li>• copying words or ideas from someone else without giving credit</li> <li>• failing to put a quotation in quotation marks</li> <li>• giving incorrect information about the source of a quotation</li> <li>• changing words but copying the sentence structure of a source without giving credit</li> </ul>

- 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](http://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. The reading materials will be provided by the instructor, at the relevant week.

<b>TENTATIVE COURSE OUTLINE</b>			
<b>Week</b>	<b>Topics</b>	<b>Readings</b>	<b>Assignments, quizzes, and exams</b>
Week 1 23.09-27.09	Introduction to Cryptography	Chapter 1.1, 1.2, 1.3	
Week 2 30.09-4.10	Modular Arithmetic and Historical Ciphers	Chapter 1.4	
Week 3 7.10-11.10	Stream Ciphers and Random Numbers	Chapter 2.1, 2.2.2.1, 2.2.2, 2.3	
Week 4 14.10-18.10	Block Ciphers and DES	Chapter 3.1, 3.2, 3.3, 3.4, 3.5	
Week 5 21.10-25.10	Advanced Encryption Standard	Chapter 4.1, 4.2, 4.3, 4.4	<b>Assignment 1</b> <b>(Due : 27.10.2024 )</b>

Week 6 28.10-1.11	Block Cipher Operations (No lecture for Sect.1 – National Holiday on 29.10)	Chapter 5.1.1, 5.1.2, 5.1.3	<b>Quiz1</b>
Week 7 4.11-8.11	Block Cipher Operations		<b>Midterm</b> <b>(9.11.2024 Saturday 15:00-17:00)</b>
Week 8 11.11-15.11	Introduction to Public-Key Cryptography	Chapter 6.1, 6.2	
Week 9 18.11-22.11	Number Theory for Public-Key Cryptography	Chapter 6.3	
Week 10 25.11-29.11	RSA Cryptosystem	Chapter 7.1, 7.2, 7.3, 7.4	
Week 11 2.12-6.12	Diffie- Hellman Key Exchange and Discrete Log Problem	Chapter 8.1, 8.3, 8.4	
Week 12 9.12-13.12	Digital Signatures	Chapter 10.1, 10.2	<b>Assignment 2</b> <b>(Due : 15.12.2024 )</b>
Week 13 16.12-20.12	Hash Functions &	Chapter 11.2, 11.4,12.1, 12.2	
Week 14 23.12-27.12	Message Authentication Codes	Chapter 12.1, 12.2	<b>Quiz 2</b>

<b>Prepared By &amp; Date</b>	Dr. Elif KURTARAN ÖZBUDAK 23/09/2024	<b>Revision Date</b>	
-------------------------------	--	----------------------	--

## **STUDENT SERVICES INFO:**

### **Student Development and Psychological Counseling Center:**

The Center is a service mandated with providing crisis intervention and supportive listening services to the campus community. A major part of fulfilling that mandate is raising awareness of our service so students know they are never alone in dealing with problems. You may contact the SDPCC at: [ogrencidanismamerkezi@tedu.edu.tr](mailto:ogrencidanismamerkezi@tedu.edu.tr), 0312 585 0316, Office A122, Or visit their website at <http://csc.tedu.edu.tr/>

### **TEDU COPeS - Psycho-Social Support**

TED University Psychosocial Support Team was initially established in order to facilitate coping with the psychological, social, familial, academic, and professional difficulties that may arise due to adverse conditions associated with COVID-19 pandemic for TEDU students and employees.

In time we have expanded our services to provide psychosocial support in diverse disasters. In this line, TEDU COPeS offers psychosocial support for TED University students and employees in the aftermath of Kahramanmaraş earthquakes.

For further information and/or questions, visit their website at <https://copes.tedu.edu.tr/>

### **Specialized Support and Students with Disabilities**

Students who may require specialized support due to a disability affecting mobility, vision, hearing, learning, mental or physical health should consult with Specialized Support and Disability Coordinator, Asst. Prof. Emrah Keser E-mail: [emrah.keser@tedu.edu.tr](mailto:emrah.keser@tedu.edu.tr), or visit the website at <https://www.tedu.edu.tr/tr/main/engelsiz-tedu>