<table>
<tr><th colspan="2">COURSE DESCRIPTION FORM</th></tr>
<tr><td>Course Code and Name</td><td>CENG475 INTRODUCTION TO CRYPTOGRAPHY (TECH.ELECT.)</td></tr>
<tr><td>Course Semester</td><td>7</td></tr>
<tr><td>Catalogue Data of the Course (Course Content)</td><td>Fundamentals of cryptographic and encryption systems, Classic Cryptography systems and numeric theory, symmetric and asymmetric algorithms, data cryptography standards (DES), advanced cryptography standards (AES), keys, key management and public keys, RSA algorithm, hashing algorithms, cryptographic protocols</td></tr>
<tr><td>Course Textbooks</td><td>D. R. Stinson, Cryptography: theory and practice, 3rd edition, CRC, 2005.</td></tr>
<tr><td>Supplementary Textbooks</td><td>Introduction to Modern Cryptography: Principles and Protocols, J. Katz, Y. Lindell, CRC, 2007.
Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Bruce Schneier, 1996.</td></tr>
<tr><td>Credit (ECTS)</td><td>6</td></tr>
<tr><td>Prerequisites for the Course (Attendance Requirements)</td><td>There is no prerequisite or co-requisite for this course.</td></tr>
<tr><td>Course Type</td><td>Technical Elective</td></tr>
<tr><td>Language of Instruction</td><td>English</td></tr>
<tr><td>Course Objectives</td><td>Teaching the fundamentals of cryptography, encryption systems and algorithms.</td></tr>
<tr><td>Course Learning Outcomes</td><td>1. Ability to understand cryptographic algorithms, techniques and mathematics behind them
2. Ability to use cryptographic algorithms
3. Ability to choose suitable cryptographic algorithms
4. Ability to have an idea about key infrastructure</td></tr>
<tr><td>Instruction Method
(Face-to-face, Distance education etc.)</td><td>The mode of delivery of this course is face to face.</td></tr>
<tr><td>Weekly Schedule of the Course</td><td>1. Week: Cryptography and encryption systems, the basic concepts
2. Week: Classical cryptographic systems and number theory
3. Week: Symmetric and asymmetric algorithms
4. Week: Symmetric and asymmetric algorithms
5. Week: Data encryption standard (DES)
6. Week: Advanced encryption standard (AES)
7. Week: Keying
8. Week: Key management and public key
9. Week: RSA algorithm
10. Week: RSA algorithm
11. Week: Hashing algorithms
12. Week: Hashing algorithms
13. Week: Cryptographic protocols
14. Week: Cryptographic protocols</td></tr>
<tr><td>Teaching Activities
(The time spent for the activities listed here will determine the amount of credit required)</td><td>Weekly theoretical course hours: 3
Reading activities
Internet search and library work
Designing and implementing materials
Midterm and revision for midterm
Final exam and revision for final exam</td></tr>
<tr><td>Assessment Criteria</td><td>
<table>
<tr><th></th><th>Number(s)</th><th>Weight (%)</th></tr>
<tr><td>Midterm exam</td><td>1</td><td>30</td></tr>
<tr><td>Assignment</td><td>2</td><td>30</td></tr>
<tr><td>Application</td><td>0</td><td></td></tr>
<tr><td>Project</td><td>0</td><td></td></tr>
</table>
</td></tr>
</table>

	Practice	0	
	Quiz	0	
	Final exam	1	40
	Total	4	100

Workload of the Course

Activity	Number of Weeks	Duration (Weekly Hour)	End of Semester Total Workload
Weekly theoretical course hours	14	3	42
Weekly practical course hours			0
Reading activities	14	2	28
Internet search and library work	12	2	24
Designing and implementing materials	2	8	16
Making a report			0
Preparing and making presentations			0
Midterm and revision for midterm	1	15	15
Final exam and revision for final exam	1	20	20
Total workload			145
Total workload/ 25			5.8
Course Credit (ECTS)			6

Contribution Level between Course Outcomes and Program Outcomes

No	Program Outcomes	1	2	3	4	5
1	Knowledge of mathematics, science, basic engineering, computing, and computer engineering; ability to use this knowledge in solving complex engineering problems.				X	
2	Ability to define, formulate and analyze complex engineering problems using basic science, mathematics and engineering knowledge and considering the UN Sustainable Development Goals relevant to the problems addressed.					X
3	Ability to design creative solutions to complex engineering problems; ability to design complex systems, processes, devices, software, algorithms or products to meet current and future requirements, considering realistic constraints and conditions.					X
4	Ability to select, use and develop appropriate techniques, resources and modern engineering and informatics tools, including estimation and modeling, for the analysis and solution of complex engineering problems while being aware of their limitations.			X		
5	Ability to use research methods to examine complex engineering problems or research topics in computer engineering, including reviewing the literature, designing experiments, conducting experiments, collecting data, analyzing and interpreting results.			X		
6	Knowledge of the effects of engineering practices and the standards used in these practices on society, health and safety, economy, sustainability and environment within the scope of the UN Sustainable Development Goals; awareness of the consequences of engineering solutions in the fields of information security and law.					X
7	Acting in accordance with engineering					

	professional principles and knowledge on ethical responsibility; awareness of acting impartially, without discrimination on any issue, and being inclusive of diversity.						
8	Ability to work effectively individually and as a team member or leader in intradisciplinary and multidisciplinary teams (face-to-face, remote, or hybrid).						
9	Ability to conduct effective verbal and written communication on technical issues in Turkish or English, prepare reports, make effective presentations and prepare software documentation, considering the various differences of the target audience (such as education, language, profession).				X		
10	Knowledge of business practices such as project, risk and change management and economic feasibility analysis; awareness of entrepreneurship and innovation.						
11	Lifelong learning skill that includes the ability to learn independently and continuously, to adapt to new and developing scientific practices and technologies, and to think inquisitively about technological changes.					X	

Lecturer(s) and Contact Information	Lecturer Dr. Muhammet Ünal muhunal@gazi.edu.tr