<table>
<tr><th colspan="2">COURSE DESCRIPTION FORM</th></tr>
<tr><td>Course Code and Name</td><td>CENG468 E-SIGNATURE AND PUBLIC KEY INFRASTRUCTURE (TECH. ELECT.)</td></tr>
<tr><td>Course Semester</td><td>8</td></tr>
<tr><td>Catalogue Data of the Course (Course Content)</td><td>Ensuring reliable communication in the network environment, authentication, non-repudiation, e-signature standards and algorithms, public key infrastructure software and hardware, e-signature legislation</td></tr>
<tr><td>Course Textbooks</td><td>Digital Signatures (Advances in Information Security), Jonathan Katz, Springer, 2010</td></tr>
<tr><td>Supplementary Textbooks</td><td>- Introduction to Public Key Infrastructures, Book by Alexander Wiesmaier, Evangelos Karatsiolis, and Johannes Buchmann, Springer, 2013
- Public Key Infrastructure: Building Trusted Applications and Web Services, Book by John R. Vacca, Auerbach Publications, 2014</td></tr>
<tr><td>Credit (ECTS)</td><td>6</td></tr>
<tr><td>Prerequisites for the Course (Attendance Requirements)</td><td>-</td></tr>
<tr><td>Course Type</td><td>Elective</td></tr>
<tr><td>Language of Instruction</td><td>English</td></tr>
<tr><td>Course Objectives</td><td>To carry out a comprehensive review of the basic concepts, algorithms, applications, software, hardware and legislation related to e-signature and public key infrastructure.</td></tr>
<tr><td>Course Learning Outcomes</td><td>Students taking this course
1. Understand the importance of the concepts of authentication and non-repudiation.
2. Know e-signature standards and legislation.
3. Analyze e-signature algorithms.
4. Use public key infrastructure software and hardware.</td></tr>
<tr><td>Instruction Method
(Face-to-face, Distance education etc.)</td><td>Face-to-face</td></tr>
<tr><td>Weekly Schedule of the Course</td><td>Week 1: E-signature definition, components, applications
Week 2: Security attributes, data integrity
Week 3: Authentication and non-repudiation
Week 4: Hash algorithms
Week 5: Computer and communication security
Week 6: Attacks
Week 7: Standards, ISO 27001
Week 8: Keys, public key concept
Week 9: Digital signature algorithms
Week 10: Certificates
Week 11: Public key infrastructure and components
Week 12: E-signature software and hardware
Week 13: E-signature software and hardware
Week 14: E-Signature Law, E-signature applications</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
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>3</td><td>30</td></tr>
<tr><td>Application</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Project		
Practice		
Quiz		
Final exam		40
Total		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			
Reading activities	12	4	48
Internet search and library work	10	3	30
Designing and implementing materials			
Making a report			
Preparing and making presentations			
Midterm and revision for midterm	1	15	15
Final exam and revision for final exam	1	15	15
Total workload			150
Total workload/ 25			6
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).					
	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	Assoc. Prof. Dr. Mehmet DEMİRCİ mdemirci@gazi.edu.tr						