Course Description Form

Course Code and Name	CENG475 INTRODUCTION TO CRYPTOGRAPHY (TECH.ELECT.)
Course Semester	7
Catalog Content	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
Textbook	D. R. Stinson, Cryptography: theory and practice, 3rd edition, CRC, 2005.
Supplementary Textbooks	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.
Credit	6
Prerequisites of the Course **(** *Attendance Requirements***)**	There is no prerequisite or co-requisite for this course.
Type of the Course	Technical Elective
Instruction Language	English
Course Objectives	Teaching the fundamentals of cryptography, encryption systems and algorithms.
Course Learning Outcomes	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
Instruction Methods	The mode of delivery of this course is face to face.
Weekly Schedule	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
Teaching and Learning Methods *(These are examples. Please fill which activities you use in the course)*	Weekly theoretical course hours: 3 Reading Activities Internet browsing, library work Designing and implementing materials Preparation of Midterm and Midterm Exam Final Exam and Preparation for Final Exam

Assessment Criteria

	Numbers	**Total Weighting (%)**
Midterm Exams	1	30
Assignment	2	30
Application	0	
Projects	0	
Practice	0	

Quiz	0		
Percent of In-term Studies (%)		60	
Percentage of Final Exam to Total Score (%)		40	
Attendance			

Workload

Activity	Total Number of Weeks	Duration (weekly hour)	Total Period Work Load
Weekly Theoretical Course Hours	14	3	42
Weekly Tutorial Hours			0
Reading Tasks	14	2	28
Studies	12	2	24
Material Design and Implementation	2	8	16
Report Preparing			0
Preparing a Presentation			0
Presentations			0
Midterm Exam and Preparation for Midterm Exam	1	15	15
Final Exam and Preparation for Final Exam	1	20	20
Other (should be emphasized)			0
Total Workload			145
Total Workload / 25			5.8
Course Credit (ECTS)			6

Contribution Level Between Course Learning Outcomes and Program Outcomes

No	Program Outcomes	1	2	3	4	5
1	Sufficient knowledge on mathematics, science and computer engineering; ability to apply theoretical and practical knowledge in these areas to model and solve engineering problems			X		
2	Ability to identify, define, formulate and solve complex engineering problems; ability to choose and apply appropriate analysis and modelling methods for these purposes	X				
3	Ability to design a complex system, process, device, software, algorithm, or product under realistic constraints and circumstances to meet certain requirements; ability to apply modern design techniques for this purpose	X				
4	Ability to choose, develop and use modern techniques and tools necessary for engineering applications; ability to effectively use computing technologies			X		
5	Ability to design and implement systems or experiments to solve engineering problems, collect and interpret data to evaluate and analyze the results of solutions		X			
6	Ability to work effectively in intradisciplinary and interdisciplinary teams or individually	X				
7	Ability to efficiently prepare, evaluate and interpret reports					X
8	Ability to make presentations and conduct effective verbal and written communication in Turkish and English	X				

	9	Awareness of the necessity of lifelong learning; ability to access information, follow scientific and technological developments; ability to perpetually renew oneself			X		
	10	Awareness of professional and ethical responsibility, ability to act in accordance with ethical principles		X			
	11	Ability to apply knowledge on project management, risk management and change management	X				
	12	Awareness of entrepreneurship and innovation, ability to design and build sustainable systems		X			
	13	Ability to devise local and global solutions to contemporary issues considering the effects of engineering applications on health, environment and security				X	
	14	Awareness of the legal consequences of engineering solutions	X				
	15	Ability to apply knowledge on software development process and documentation rules	X				
	16	Knowledge on standards used in engineering applications				X	
	17	Awareness of occupational health and security, information security and privacy				X	
The Course's Lecturer(s) and Contact Information	Lecturer Dr. Muhammet Ünal muhunal@gazi.edu.tr						