İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Ağ Güvenliği	Network Security

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 501E	Güz/Bahar (Fall/Spring)	3	7,5	Y.L. (M.Sc.)

Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	İngilizce/Türkçe (English/Turkish)

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	İnternet güvenliği. Güvenlik standartları. Yabancılar ve virüsler. E-posta güvenliği. Simetrik ve asimetrik kriptografi. Kriptografik özler. Asıllama sistemleri. Sayısal imzalar. Sayısal sertifikalar. Güncel ağ güvenliği konuları ve yayınları.
	Web security. Security standards. Intruders and viruses. E-mail security. Firewalls. Secret Key and Public/Private Key Cryptography Cryptographic Hashes and Message Digests Authentication Systems. Digital signatures and certificates. Digital certificates. Current Network Security Topics and Publications.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	• Ağ yapısını tanıtmak • Ağa yapılabilecek saldırıları sınıflandırmak ve genellikle bilinen önlemleri belirlemek • Şifreleme yöntemlerini öğretmek • Bir ağ alanına içeriden yapılabilecek saldırıları tanımak
	• Introduction to network topology • Classification of attacks to networks and defining of protection • To teach encryption methods • To recognize internal frauds
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Öğrenciler güvenliğin neden gerektiğini kavrayacaklar. 2. Öğrenciler sık karşılaşılan saldırıları ve önlemleri tanıyacaklar. 3. Öğrenciler şifreleme yöntemleri konusunda fikir sahibi olacaklar. 4. Öğrenciler şifreleme yöntemlerinin kullanılabileceği alanlarla ilgili fikir edinecekler.
	1. Students will understand the necessity of security 2. Understanding of common attacks and counter measures 3. Understanding of encryption methods. 4. Understanding the usage of encryption methods.

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1. Network Security Essentials Applications and Standards, 5th Ed., William Stallings, 2013, Prentice Hall. 2. Network Security Bible, 2nd Ed., Eric Cole, 2009, Wiley. 3. Cryptography and Network Security: Principles and Practice, 6th Ed., William Stallings, 2013, Prentice Hall. 4. Network Security Essentials: Applications and Standards, 4th Ed., William Stallings, 2010, Prentice Hall. 5. Network Security: The Complete Reference, Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg, 2003, McGraw-Hill Osborne Media.
Ödevler ve Projeler **(Homework & Projects)**	1 Dönem Ödevi 1 Term Paper
Laboratuar Uygulamaları **(Laboratory Work)**	-- --
Bilgisayar Kullanımı **(Computer Use)**	-- --
Diğer Uygulamalar **(Other Activities)**	-- --

Başarı Değerlendirme Sistemi

(Assessment Criteria)

Faaliyetler (Activities)	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
Yıl İçi Sınavları (Midterm Exams)	1	% 30 (30 %)
Kısa Sınavlar (Quizzes)	-	-
Ödevler (Homework)	-	-
Projeler (Projects)	-	-
Dönem Ödevi/Projesi (Term Paper/Project)	1	% 30 (30%)
Laboratuar Uygulaması (Laboratory Work)	-	-
Diğer Uygulamalar (Other Activities)	-	-
Final Sınavı (Final Exam)	1	% 40 (40%)

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Ağ güvenliği kavramları	
2	Yabancı yazılımlar ve virüsler	
3	Bakışımlı şifreleme	
4	Bakışımsız şifreleme	
5	Öz alma ve elektronik imza	
6	Sertifikalar ve açık anahtar altyapısı	
7	Asıllama	
8	Erişim denetimi	
9	Denetlenebilirlik	
10	Ağ izleme ve güvenlik duvarları	
11	Sızma önleme ve saldırgan yanıltma yöntemleri	
12	Güncel konular	
13	Güncel yayınlar	
14	Güncel yayınlar	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	The concept of network security	
2	Malwares and viruses	
3	Symmetric encryption	
4	Asymmetric encryption	
5	Hashing and electronic signatures	
6	Certificates and PKI	
7	Authentication	
8	Access control	
9	Auditability	
10	Network monitoring and firewalls	
11	Intrusion detection and honeypots	
12	Case studies	
13	Paper review	
14	Paper review	

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).	X		
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).		X	
iii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).			
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).	X		
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).			
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).		X	
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).	X		
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).	X		

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (MS) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).	X		
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).		X	
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).			
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).	X		
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).			
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).			
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).		X	
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).	X		
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).	X		

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Prof. Dr. Eşref ADALI	31.03.2014	