

**İTÜ**  
**LİSANSÜSTÜ DERS KATALOG FORMU**  
**(GRADUATE COURSE CATALOGUE FORM)**

<b>Dersin Adı</b>			<b>Course Name</b>		
E-Ticarette Güvenlik			E-Commerce Security		
<b>Kodu (Code)</b>	<b>Yarıyılı (Semester)</b>	<b>Kredisi (Local Credits)</b>	<b>AKTS Kredisi (ECTS Credits)</b>	<b>Ders Seviyesi (Course Level)</b>	
BGK 509	Güz/Bahar (Fall/Spring)	3	7,5	Y.L. (M.Sc.)	
<b>Lisansüstü Program (Graduate Program)</b>	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)				
<b>Dersin Türü (Course Type)</b>	Seçmeli (Elective)		<b>Dersin Dili (Course Language)</b>	Türkçe/İngilizce (Turkish/English)	
<b>Dersin İçeriği (Course Description)</b>	<p>Geçmişten günümüze ticaret. Ticaretin temel kuralları: Karşılıklı kazanım, Güvenli alışveriş ortamı, Tarafların birbirine güveni, e-ticarette güvenliği sağlama yöntemleri : Şifreleme: Şifrelemenin temelleri, Şifreleme yöntemleri, Güvenli işlemler, Genel anahtar altyapıları, kimlik doğrulama ve yetkilendirme belgeleri, güvenli kimlik hizmetleri ve rol tabanlı yetkilendirme, elektronik ödeme sistemleri, fikri mülkiyet koruması, e-noter ve tek kullanımlık parola.</p> <p><u>30-60 kelime arası</u></p> <p>History of commerce, basic rules of commerce, mutual benefits, secure commercial markets, mutual trust, security methods for e-commerce, encryption, principles of encryption, secure transactions, PKI, identity verification and authorization documents, secure identity services and role-based authorization, electronic payment systems, protection of intellectual properties, e-notary, one time passwords.</p>				
<b>Dersin Amacı (Course Objectives)</b>	<ul style="list-style-type: none"><li>E-ticaret konusunu anlatmak</li><li>Piyasaların güvenlik algısını ve gereksinimlerini göstermek</li><li>Finansal güvenlik araçlarını tanıtmak</li></ul> <ul style="list-style-type: none"><li>To teach the concept of e-commerce</li><li>To point the safety perception and requirements of markets</li><li>Introduction to security tools for financial applications</li></ul>				
<b>Dersin Öğrenme Çıktıları (Course Learning Outcomes)</b>	<ol style="list-style-type: none"><li>Öğrenciler e-ticaret ve gereksinimlerini öğrenecekler.</li><li>Öğrenciler finansal güvenlik araçlarını tanıyacaklar.</li><li>Öğrenciler güven ilişkileri konusunda bilgi kazanacaklar.</li><li>Öğrenciler finansal dünyanın gerektirdiği yeni kavramları güvenlik ilkeleriyle karşılamayı öğrenecekler.</li></ol> <ol style="list-style-type: none"><li>To teach requirements of e-commerce</li><li>To teach security tools for financial applications</li><li>To teach topics of mutual trust</li><li>Up-to-date topics of the financial world</li></ol>				

<b>Kaynaklar</b> (References) <i>En önemli 5 adedini belirtiniz</i>	<ol style="list-style-type: none"> <li>1. Web Commerce Security: Design and Development, Hadi Nahari, Ronald L. Krutz, 2011, Wiley.</li> <li>2. Web Security, Privacy and Commerce, 2nd Ed., Simson Garfinkel, 2002, O'Reilly Media.</li> <li>3. Electronic Commerce, 10th Ed., Gary Schneider, 2012, Cengage Learning.</li> <li>4. Essentials of Online payment Security and Fraud Prevention, David A. Montague, 2010, Wiley.</li> <li>5. E-Commerce Security: Weak Links, Best Defenses, Anup K. Ghosh, 1998, Wiley.</li> </ol>		
<b>Ödevler ve Projeler</b> (Homework & Projects)	1 Dönem Ödevi		
	1 Term Paper		
<b>Laboratuvar Uygulamaları</b> (Laboratory Work)	--		
	--		
<b>Bilgisayar Kullanımı</b> (Computer Use)	--		
	--		
<b>Diğer Uygulamalar</b> (Other Activities)	--		
	--		
<b>Başarı Değerlendirme Sistemi</b> (Assessment Criteria)	<b>Faaliyetler</b> (Activities)	<b>Adedi*</b> (Quantity)	<b>Değerlendirmedeki Katkısı, %</b> (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%)
	Laboratuvar 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	Dersin kapsamı	
2	Ticaretin temel konuları	
3	Karşılıklı kazanım ilkesi	
4	Ticarette güvenlik gereksinimi	
5	Güvenli ticaretin şartları	
6	Güven ilişkileri	
7	Şifreleme yöntemleri	
8	Şifreleme yöntemleri	
9	Asıllama ve yetkilendirme	
10	Elektronik ödeme dizgeleri	
11	Fikri mülkiyet	
12	E-noter kavramı	
13	Güvenli e-ticaret dizgeleri	
14	Güncel uygulamalar	

## COURSE PLAN

Weeks	Topics	Course Outcomes
1	Course contents	
2	Basic topics of commerce	
3	Principle of mutual benefit	
4	Requirements of security for commerce	
5	Condition of secure commerce	
6	Trust relations	
7	Encryption methods	
8	Encryption methods	
9	Authentication and authorization	
10	Electronic payment systems	
11	Intellectual properties	
12	Concept of e-notary	
13	Secure e-commerce systems	
14	Modern applications	

## Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracığı 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).			X
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 çözümlenebilir (beceri).		X	
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 öngörülemez 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 özümledikleri 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).			X
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).		X	
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**

<u><i>Düzenleyen (Prepared by)</i></u> Prof. Dr. Eşref ADALI	<u><i>Tarih (Date)</i></u> 31.03.2014	<u><i>İmza (Signature)</i></u>
---	--	--------------------------------