

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

<b>Dersin Adı</b>		<b>Course Name</b>		
Bilgi Güvenliği ve Savunma için Uygulamalı Şifreleme		Applied Cryptography for Cyber security and Defense		
<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 604	Güz/Bahar (Fall/Spring)	3	7,5	Dr. (Ph.D.)
<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>	Siber güvenlik ve şifreleme temel tanımları, Bilgi güvenliği sistemlerinin korunması için şifreleme tabanlı kimlik denetimi uygulamaları, e-mail, web servisleri ve şifreleme uygulamaları, Elektronik ticarete şifreleme uygulamaları, Telsiz duyarga ağlarında uygulamalı şifreleme, Güvenilir elektronik oylama protokolleri, Ağ güvenliği ve şifreleme ile önlemler, Şifreleme protokolleri ve yazılım/donanım uygulamaları <i>30-60 kelime arası</i>			
	Cyber security. Encryption. Authentication based on encryption to protect information security systems. Encryption in web and e-mail systems. Encryption in e-commerce. Encryption in sensor networks. Electronic voting protocols. Network security. Encryption methods and hardware software applications.			
<b>Dersin Amacı (Course Objectives)</b>	<ul style="list-style-type: none"><li>Şifreleme yöntemlerinin gerçek sistemlere uygulanması ve deneyim kazanılması</li><li>Güvenli bir altyapının temel bileşenlerinin uygulamalı olarak tümleştirilmesi</li></ul>			
	<ul style="list-style-type: none"><li>Application of cryptographic methods to real systems and gaining experience</li><li>Integrating components of a secure infrastructure</li></ul>			
<b>Dersin Öğrenme Çıktıları (Course Learning Outcomes)</b>	1. Öğrenciler güvenli bir uygulama altyapısı için gereken işlevleri belirleyecek 2. Bu işlevleri gerçekleyecek 3. Bu işlevlere dayanarak çözüme yönelik bir uygulama tasarlayacak 4. Tasarlanan uygulama gerçekleştirilerek deneyim kazanılacaktır.			
	1. Determining required functionality for a secure infrastructure 2. Implementing these functionality 3. An application will be designed based on implemented functionality 4. The application will be implemented			

<b>Kaynaklar</b> (References) <i>En önemli 5 adedini belirtiniz</i>	<ol style="list-style-type: none"> <li>1. Cybersecurity and Cyberwar: What Everyone Needs to Know, P.W. Singer, Allan Friedman, 2014, Oxford University Press.</li> <li>2. Managing Risk In Information Systems, Darril Gibson, 2010, Jones &amp; Bartlett Learning.</li> <li>3. Accounting Information Systems, 9th Ed., Ulric J. Gelinas, Richard B. Dull, Patrick Wheeler, 2011, Cengage Learning.</li> <li>4. Principles of Information Systems Security: Texts and Cases, Gurpreet Dhillon, 2006, Wiley.</li> <li>5. Management of Information Security, 4th Ed., Michael E. Whitman, Herbert J. Mattord, 2013, Cengage Learning.</li> </ol>		
<b>Ödevler ve Projeler</b> (Homework & Projects)	1 Dönem Ödevi		
	1 Term Paper		
<b>Laboratuar 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%)
	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	Derse giriş, siber güvenliğin tanımı ve kapsamı	
2	Uygulamalı asıllama yöntemleri	
3	Uygulamalı asıllama yöntemleri	
4	Erişim ilkelerinin belirlenmesi	
5	Farklı yetkilendirme yöntemleri ile ilkelerin dayatılması	
6	Erişimin izlenmesi ve raporlanması	
7	Uzaktan erişim için güvenli haberleşme protokollerinin kurulması	
8	Seçilen bir uygulamanın geliştirilmesi: gerekliliklerin belirlenmesi	
9	Seçilen bir uygulamanın geliştirilmesi: gerekli temel şifreleme yapılarının belirlenmesi, donanımsal yapıların temini ve yazılımsal yapıların gerçekleştirilmesi	
10	Seçilen bir uygulamanın geliştirilmesi: uygulamanın modellenmesi ve tasarımı	
11	Seçilen bir uygulamanın geliştirilmesi: uygulamanın kodlanması	
12	Seçilen bir uygulamanın geliştirilmesi: uygulamanın kodlanması	
13	Seçilen bir uygulamanın geliştirilmesi: uygulamanın sınanması	
14	Tartışmalar	

## COURSE PLAN

Weeks	Topics	Course Outcomes
1	Cyber security and its coverage	
2	Applied authentication methods	
3	Applied authentication methods	
4	Determining access rules	
5	Enforcing access rules with a set of access control methods	
6	Monitoring and reporting access	
7	Secure communication protocols for remote access	
8	Developing an application: Determining requirements	
9	Developing an application: determining required cryptographic primitives, hardware and software components	
10	Developing an application: Modelling and design	
11	Developing an application: Implementation	
12	Developing an application: Implementation	
13	Developing an application: Testing	
14	Discussion	

## Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Doktora 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).			X
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).		X	
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			X
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).	X		
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 (PhD) 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).			X
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).		X	
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)			X
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).	X		
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**

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