

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

<b>Dersin Adı</b>				<b>Course Name</b>	
Bilgi Güvenliği alanında Veri Madenciliği Yöntemleri				Data Mining Methods in 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 510	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/İngilice (Turkish/English)
<b>Dersin İçeriği (Course Description)</b>		Veri madenciliği konusunun temelleri, Veri temizleme, Veri modelleme, İlişkilendirme Kuralları, Sınıflandırma, Kümeleme ve Demetleme algoritmaları ve bunların uygulamaları. Bu yöntemlerin bilgi güvenliği alanında kullanım olanakları ve yöntemleri			
<u>30-60 kelime arası</u>		Fundamentals of data mining, data cleaning, data modelling, relation rules, classification, clustering and aggregation algorithms and their applications. Application of data mining topics to information security.			
<b>Dersin Amacı (Course Objectives)</b>		<ul style="list-style-type: none"><li>• Veri madenciliğini tanıtmak</li><li>• Veri madenciliği yöntemlerini öğretmek</li><li>• Veri madenciliği yöntemleri ile bir saldırı örüntüsünü saptamak</li></ul>			
<u>Maddeler halinde 2-5 adet</u>		<ul style="list-style-type: none"><li>• Introducing data mining</li><li>• Teaching data mining methods</li><li>• Detecting an attack pattern with data mining tools</li></ul>			
<b>Dersin Öğrenme Çıktıları (Course Learning Outcomes)</b>		Öğrenciler			
<u>Maddeler halinde 4-9 adet</u>		<ol style="list-style-type: none"><li>1. Veri madenciliğini tanıyacaklardır.</li><li>2. Veri madenciliğinin temel ilkelerini öğreneceklerdir.</li><li>3. Veri madenciliği ilkeleriyle bir saldırıyı uygulamalı olarak saptayacaklardır.</li><li>4. Konunun güncel örnekleri üzerine akıl yürütecek ve tartışacaklardır.</li></ol>			
		<ol style="list-style-type: none"><li>1. Data mining concept will be thought</li><li>2. Principles of data mining will be thought</li><li>3. An attack will be experimentally detected with data mining tools</li><li>4. Recent academic discussion will be conducted</li></ol>			

<b>Kaynaklar</b> (References) <i>En önemli 5 adedini belirtiniz</i>	<ol style="list-style-type: none"> <li>1. Data Mining: Concepts and Techniques, 3rd Ed., Jiawei Han, Micheline Kamber, 2011, Morgan Kaufmann.</li> <li>2. Data Mining: Practical Machine Learning Tools and Techniques, 3rd Ed., Ian H. Witten, Eibe Frank, Mark A. Hall, 2011, Morgan Kaufmann.</li> <li>3. Machine Learning and Data Mining for Computer Security: Methods and Applications, 2006 Ed., Marcus A. Maloof, 2012, Springer.</li> <li>4. Privacy Preserving Data Mining, 2006 Ed., Jaideep Vaidya, Christopher W. Clifton, Yu Michael Zhu, 2005, Springer.</li> <li>5. Investigative Data Mining for Security and Criminal Detection, Jesus Mena, 2002, Butterworth-Heinemann.</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 (Activities)</b>	<b>Adedi* (Quantity)</b>	<b>Değerlendirmedeki Katkısı, % (Effects on Grading, %)</b>
	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	Giriş	
2	Veri madenciliğinin temelleri	
3	Veri süzme ve temizleme	
4	Veri modelleme	
5	Veri ilişkilendirme yöntemleri	
6	Veri sınıflandırma	
7	Kümeleme ve demetleme algoritmaları	
8	Saldırı örüntülerinin modellenmesi	
9	Saldırı örüntülerini tanımlanması sınıflandırılması	
10	Saldırıları örüntülerini belirleme	
11	Güncel uygulamalar	
12	Güncel yayınlar ve tartışma	
13	Güncel yayınlar ve tartışma	
14	Güncel yayınlar ve tartışma	

## COURSE PLAN

Weeks	Topics	Course Outcomes
1	Introduction	
2	Foundations of data mining	
3	Data filtering and cleaning	
4	Data modelling	
5	Data relation methods	
6	Data classification	
7	Clustering and aggregation algorithms	
8	Modelling attack patterns	
9	Defining and classifying attack patterns	
10	Detecting attack patterns	
11	Up-to-date applications	
12	Recent literature reviews and discussion	
13	Recent literature reviews and discussion	
14	Recent literature reviews and discussion	

## 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 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).	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 (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).	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>
-----------------------------------------------------------------	------------------------------------------	--------------------------------