

İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı				Course Name	
Bilgisayar Ağlarında Güvenlik				Security in Computer Networks	
Kodu (Code)	Yarıyılı (Semester)	Kredisi (Local Credits)	AKTS Kredisi (ECTS Credits)	Ders Türü (Course Type)	
BLG510E	II Bahar	3	7,5	Seçmeli (Elective)	
Bölüm / Program (Department/Program)		Bilgisayar Mühendisliği / Computer Engineering			
Dersin Türü (Course Type)		Seçmeli (Elective)		Dersin Dili (Course Language)	İngilizce (English)
Dersin İçeriği (Course Description)		Sayılar teorisi, Bilgisayar ağları, Bilgisayar güvenliği kavramları, Kriptoloji, Ağ ve taşıma katmanında güvenlik, Asıllama ve yetkilendirme yöntemleri, Güvenlik uygulamaları: Sanal özel ağ, Sızma belirleme sistemi, Güvenlik duvarı, Virüs tarayıcı, Bulut ve nesnelerin İnterneti için güvenlik.			
		Number theory, Computer networks, Computer security concepts, Cryptology, Security in network and transport layers, Authentication and authorization methods, Security applications: VPNs, IDSs, Firewalls, Virus scanners, Security in the cloud and IoT.			
Dersin Amacı (Course Objectives)		1. Ağ güvenliği ve kriptoloji konularını öğretmek 2. Öğrencilerin bilgisayar ağlarının ve sistemlerinin güvenliğini anlamalarını ve çözümleyebilmelerini sağlamak 3. Öğrencilerin güvenlik mimarileri tasarlayabilmelerini sağlamak 4. Uygulamada karşılaşılan güvenlik kavramlarını göstermek: tehditler, zayıflıklar, saldırılar ve saldırı savuşturma dizgeleri 5. Yasal konuları tartışmak			
		1. To teach network security and cryptography 2. To make the students understand and be able to analyze the security of computer systems and networks 3. To make the students be able to design security architectures 4. To experiment practical security: threats, vulnerabilities, attacks and attack prevention systems 5. To discuss legal issues			
Dersin Öğrenme Çıktıları (Course Learning Outcomes)		1. Kriptolojiye ilişkin bilgi sahibi olmak; kriptografik ve kriptanalitik yöntemleri tanımak 2. Güvenlik mimarilerinin bileşenlerini bir araya getirmek ya da ayrıştırmak, bileşenlerin etkileşimi hakkında akıl yürütmek 3. Güvenlik protokolü tasarlamak ve çözümlemek 4. Güvenliğe ilişkin yasal ve toplumsal konularla ilgili bilgi sahibi olmak			
		1. To have knowledge on cryptography; to be familiar with cryptographic and cryptanalytic methods 2. To Be able to compose and decompose components of security architectures, reason about the relation of components 3. To be able to analyze and design security protocols 4. To be familiar with the related social and legal issues			

Ders Kitabı (Textbook)	“Cryptography and Network Security: Principles and Practice, 7th Edition”, William Stallings, 2017, Pearson.		
Diğer Kaynaklar (Other References)	• “Thinking Security: Stopping Next Year's Hackers”, 2016, Steven M. Bellovin, Pearson. • “Introduction to Network Security: Theory and Practice, 2nd Edition”, Jie Wang, Zachary A. Kissel, 2015, Wiley. • “Network Security: Private Communications in a Public World, Second Edition”, Mike Speciner, Radia Perlman, Charlie Kaufman, 2002, Pearson. • “Network Security Essentials: Applications and Standards, 6th Edition”, William Stallings, 2016, Pearson.		
Ödevler ve Projeler (Homework & Projects)	Dersin bir dönem projesi vardır.		
	There will be one term project.		
Laboratuvar 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)	2	40
	Kısa Sınavlar (Quizzes)		
	Ödevler (Homework)		
	Projeler (Projects)	1	20
	Dönem Ödevi/Projesi (Term Paper/Project)		
	Laboratuvar Uygulaması (Laboratory Work)		
	Diğer Uygulamalar (Other Activities)		
	Final Sınavı (Final Exam)	1	40

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Güvenlik kavramı: tehditler ve hedefler. Sayılar teorisine giriş.	1, 2, 4
2	Bilgisayar Ağlarının Temelleri	2, 4
3	Klasik şifreyazım yöntemleri	1
4	Öz alma işlevleri, Mesaj asıllama kodları, şifrelemenin çalışma modları, rasgele bit oluşturma, rasgele sayı üretme, “sünger” işlevleri	1
5	Bakımsız şifreyazım: RSA ve ElGamal, Sayısal imzalar, Açık anahtar altyapısı, Vekil sertifikalar	1
6	Eliptik eğriler, Anahtar dağıtımı ve yönetimi	1
7	Özet ve güncel kriptografik gelişmeler.	1
8	Ağ katmanında güvenlik, IPSec, Taşıma katmanında güvenlik, SSL’den TLS 1.3’e, telsiz ağlarda güvenlik.	2, 3
9	Asıllama: Şifreler. Tek kullanımlık şifreler	2, 3
10	Asıllama: Tek-seferde-giriş ve kurumlararası asıllama, Kerberos, Shibboleth, sertifika tabanlı asıllama, anonim asıllama	2, 3
11	Yetkilendirme: Erişim modelleri, erişim politikaları, izinler, politikaların uygulanması için teknikler, günlükler	2, 4
12	Sanal özel ağlar, Güvenlik duvarları, Sızma belirleme sistemleri, Virüs tarayıcılar	2, 4
13	Bulut ve Nesnelerin İnterneti için güvenlik: Sanallaştırma, hesaplamayı üstleniciye bırakma, depolamayı üstleniciye bırakma, kısıtlı kaynaklarla şifreyazım teknikleri, kısıtlı enerjiyle haberleşme teknikleri	2, 3, 4
14	Özet ve güncel gelişmeler	1, 2, 3, 4

COURSE PLAN

Weeks	Topics	Course Outcomes
1	The security mindset: threats and goals. Introduction th number theory.	1, 2, 4
2	Basics of computer networks	2, 4
3	Classical cryptographic methods	1
4	Hash functions, MACs, modes of operation of encryption, random bit generation, random number generators, sponge functions	1
5	Asymmetric cryptography: RSA and ElGamal, Digital signatures, PKI, proxy certificates	1
6	Elliptic curve cryptography, Key distribution and management	1
7	Summary and recent cryptographic advancements	1
8	Security in network layer, IPSec, Security in transport layer, SSL to TLS 1.3, Security in wireless networks	2, 3
9	Authentication: passwords and OTPs	2, 3
10	Authentication: SSO and federated authentication: Kerberos & Shibboleth, certificate-based authentication, anonymous authentication	2, 3
11	Authorization: Access models, Access policies, Permissions, Policy enforcement techniques, logging	2, 4
12	VPNs, Firewalls, IDSs, Virus scanners	2, 4
13	Security in the Cloud and IoT: Virtualization and sandboxing, outsourcing execution, outsourcing storage, encryption with limited resources, networking with limited resources	2, 3, 4
14	Summary and recent advancements	1, 2, 3, 4

Dersin Bilgisayar Mühendisliği YL Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, ilgili program alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).		x	
ii.	Alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).			
iii.	Alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).		x	
iv.	Alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).		x	
v.	Alanını ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).		x	
vi.	Alanını ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	x		
vii.	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).		x	
viii.	Alanı ile ilgili sorunların çözülmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		x	
x.	Alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde 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.	Alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			x
xiii.	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.	Alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			x
xv.	Alanında özümstedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinlerarası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).		x	
xvi.	Tezli programlarda, kendi çalışmalarını, 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 the Computer Engineering Graduate (MS) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in the related program's area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).		x	
ii.	Grasping the inter-disciplinary interaction related to one's area (knowledge).			
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in the area(skill).		x	
iv.	Interpreting and forming new types of knowledge by combining the knowledge from the area and the knowledge from various other disciplines (skill).		x	
v.	Solving the problems faced in the area by making use of the research methods (skill).		x	
vi.	The ability to carry out a specialistic study related to one's 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 one's 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 the area (Competence to work independently and take responsibility)			
ix.	Assessing the specialistic 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 the area and one's own work to other groups in and out of the area; in written, oral and visual forms (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 the area (Communication and Social Competency).			x
xiii.	Paying regard to social, scientific, cultural and ethical values during the collecting, interpreting, practicing and announcing processes of the 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 the 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.	In the programs with thesis, the ability to present one's own work within the international environments orally, visually and in written forms (Area Specific Competency).	x		

<u>Düzenleyen (Prepared by)</u>	<u>Tarih (Date)</u> 21.11.2016	<u>İmza (Signature)</u>
--	--	--------------------------------