İTÜ
DERS KATALOG FORMU
(COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Ağ Güvenli ği	Network Security

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Uygulaması, Saat/Hafta (Course Implementation, Hours/Week)**		
				Ders (Theoretical)	**Uygulama (Tutorial)**	**Laboratuvar (Laboratory)**
BLG478/ BLG478E	8	2	4	2	0	0

Bölüm / Program (Department/Program)	Bilgisayar Mühendisli ği / Computer Engineering		
Dersin Türü (Course Type)	Mühendislik, Seçmeli/ Engineering, Elective	**Dersin Dili (Course Language)**	Türkçe (Turkish)/ İngilizce (English)
Dersin Önko şulları (Course Prerequisites)	BLG 433/ BLG 433E		

Dersin mesleki bileşene katkısı, % (Course Category by Content, %)	**Temel Bilimler (Basic Sciences)**	**Temel Mühendislik (Engineering Science)**	**Mühendislik Tasarım (Engineering Design)**	**İnsan ve Toplum Bilim (General Education)**
	30	50	15	5

Dersin İçeri ği **(Course Description)**	Dersin amacı, ö grencilerin bilgisayar güvenli ği, özellikle a ğ güvenli ği kavramlarına aşina olmasını sağlamaktır. Müfredat bu konuları içerir: temel güvenl ik kavramlarını, kriptografik yöntemler, eri şim kontrolü, i şletim sistemleri güvenli ği, ağ güvenli ği ve protokolleri, güvenli programlama, kötü niyetliler mantı ğı, güvenlik.
	The aim of the course is make the students be familiar with the computer security concepts, especially network security. Curriculum contains these subjects: basic security concepts, cryptographic methods, access control, operating systems security, network security and protocols, secure programming, malicious logic, safety.
Dersin Amacı **(Course Objectives)**	1. Bilgisayar güvenli ği ve kriptografi temellerini ö gretmek 2. grencilerin bilgisayar sistemleri ve ağlarının güvenli gini anlamalarını ve analiz etmelerini sağlamak 3. grencilerin güvenlik mimarileri tasarlamalarını sa ğlamak 4. grencilerin işletim sistemleri güvenlik temellerini anlamalarını sağlamak 5. grencileri güvenli programlama fikri ile tanı ştırmak
	1. Teach basics of computer security and cryptography 2. Make students be able to understand and analyze the security of computer systems and networks 3. Make students be able to design security architectures 4. Make students understand the basics of operating systems security 5. Encounter students with the idea of secure programming
Dersin Ö ğrenme Çıktıları **(Course Learning Outcomes)**	1. Güvenlik mimarileri bile şenlerini oluşturabilmek ve ayrıştırabilmek 2. Güvenlik protokollerini tasarlayabilmek ve analiz edebilmek 3. Güvenli programlama görevlerini gerçekle ştirebilmek 4. İlgili sosyal ve hukuki konular hakkında bilgi sahibi olmak
	1. Be able to compose and decompose components of security architectures 2. Be able to analyze and design security protocols 3. Be able to perform secure programming tasks 4. Be familiar with the related social and legal issues

Ders Kitabı **(Textbook)**	1. Computer Networks, Andrew S. Tanenbaum [et al.] 2. Network security fundamentals, Eric Cole [et al.]		
Diğer Kaynaklar **(Other References)**	1. Computer security : art and science, Matthew Bishop 2. Fundamentals of network security, John E. Canavan		
Ödevler ve Projeler **(Homework & Projects)**			
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)**	4	20
	Projeler **(Projects)**		
	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	1. Temel güvenlik kavramlarına giri ş 2. Kriptografiye Giriş a) Substitution and transposition ciphers, one-time pads b) Kriptografinin iki temel prensibi	1
2	3. Kriptografinin temelleri a) Hashing (bozma), bozulmuş mesaj doğrulama kodu b) Simetrik algoritmalar i. DES ii. AES iii. RC4 iv. Cipher modları	1
3	3. Kriptografinin temelleri a) Anahtar dağıtımı ve anahtar de ğişimi b) Asimetrik algoritmalar i. RSA ii. ElGamal iii. ECC	1
4	3. Kriptografinin temelleri a) Sertifikalar i. Sertifika zincirleri ii. PKI iii. Trust and public key rings	1
5	3. Kriptografinin temelleri a) İmza şemaları i. Simetrik ve asimetrik imzalama ii. Gökkü şağı tabloları iii. Doğumgünü saldırısı	1
6	4. Doğrulama Protokolleri a) Paylaşımlı sırla do ğrulama b) Anahtar dağıtım merkeziyle doğrulama c) Kerberos ile doğrulama d) Asimetrik algoritmalarla doğrulama	1, 2
7	Vize	
8	5. Haberleşme Güvenli ği a. Kesme Prensibi b. IPSec 6. Ağ Koruması a. Güvenlik Duvarları b. IDS	1, 2
9	6. Ağ Koruması a. VPN b. Kablosuz güvenlik c. DoS 7. Email güvenli ği a. PGP b. PEM	1, 2
10	7. Email Güvenli ği c. S/MIME 8. Web Güvenli ği a. Tehditler b. Güvenli isimlendirme	1, 2

11	8. Web güvenli ği a. TLS b. Mobil kod güvenli ği c. Ağda gizlilik i. Web bugs ii. Cookie ler	1, 2
12	Vize	
13	9. Yönetmelikler, yasalar ve gizlilik	4
14	10. Güvenli Programlama a. Programlama dilleri için güvenlik mimarileri b. Güvenli Programlama Prensipleri	1, 2, 3

COURSE PLAN

Weeks	Topics	Course Outcomes
1	1. Introduction to basic security concepts 2. Introduction to cryptography a. Substitution and transposition ciphers, one-time pads b. Two fundamental principles of cryptography	1
2	3. Cryptographic fundamentals a. Hashing, Hashed message authentication Code b. Symmetric algorithms i. DES ii. AES iii. RC4 iv. Cipher modes	1
3	3. Cryptographic fundamentals a. Key distribution and key exchange b. Asymmetric algorithms i. RSA ii. ElGamal iii. ECC	1
4	3. Cryptographic fundamentals a. Certificates i. Certificate chains ii. PKI iii. Trust and public key rings	1
5	4. Cryptographic fundamentals a. Signature schemes i. Symmetric and asymmetric signing ii. Rainbow tables iii. Birthday attack	1
6	5. Authentication protocols a. Authentication via shared secret b. Authentication via key distribution center c. Authentication via Kerberos d. Authentication via asymmetric algorithms	1, 2
7	Midterm	
8	6. Communication security a. Interrupt principle b. IPSec 7. Network protection a. Firewalls b. IDS	1, 2
9	8. Network protection d. VPN e. Wireless security	1, 2

	f. DoS 9. Email security a. PGP b. PEM	
10	8. Email security d. S/MIME 9. Web security a. Threats b. Secure naming	1, 2
11	9. Web security d. TLS e. Mobile code security f. Privacy in web i. Web bugs ii. Cookies	1, 2
12	Midterm	
13	10. Regulations, legislation and privacy	4
14	11. Secure programming a. Security architectures of programming languages b. Secure programming principles	1, 2, 3

Dersin Bilgisayar Mühendisli ği Programıyla İlişkisi

(1: "az", 2: "kısmi", 3: "Tam", E ğer cevabınız "Hiçbiri" ise bo ş bırakınız.)

Bilgisayar Mühendisli ği Programı Çıktıları ve Performans Ölçütleri				Katkı Seviyesi		
				1	2	3
a	**Matematik, temel bilimler ve mühendislik bilgilerin i bilgisayar mühendisli ği alanında uygulama becerisi**				x	
	a1	**Matematik, temel bilimler ve mühendislik bilgile rini edinme**			x	
		PC.a1	Matematik için soruların cevapları			
		PC.a2	Temel bilimler ve mühendislik için soruların cevapları		x	
	a2	**Matematik bilgisinin uygulanması**				x
		PC.a3	Bilgisayar mühendisli ği problemlerine analitik ve sayısal çözümler üretme de matematik ilkeleri uygulanır			x
		PC.a4	Bir probleme yönelik uygun matematiksel yöntem ya da yaklaşımlar seçilir			x
	a3	**Temel bilimler ve mühendislik esaslarına ait bilg inin uygulanması**			x	
		PC.a5	Bilgisayar mühendisli ği problemlerinin modellenmesi ve çözümünde temel bi limler ve mühendislik ilkeleri uygulanır		x	
b	**Deney tasarlayıp yürütebilme ve verileri analiz e dip yorumlama becerisi**					
	b1	**Deneyleri tasarlama**				
		PC.b1	Değişkenler, uygun ekipmanlar, test cihazları, model vb seçilir			
		PC.b2	Sonucun ya da varyantlarının değerlendirileceği etkili ölçü(ler) seçilir			
	b2	**Deneyleri yürütme**				
		PC.b3	Veri toplamak için uygun ölçme teknikleri ku llanılır			
		PC.b4	Deneyin tekrarlanabilmesi amacıyla veri toplama süreci belgelendirilir			
	b3	**Verilerin analizi**				
		PC.b5	Verileri analiz etmek için uygun araçlar (ist atistiksel ve grafiksel vb.) seçilir ve kullanılır			
	b4	**Verilerin yorumlanması**				
		PC.b6	Orijinal hipoteze göre sonuçlar yorumlanır			
c	**Bir sistemi, sistem bileşenini veya süreci; ekonomik, çevresel, sosyal, poli tik, etik, üretilebilirlik, sürdürülebilirlik, emniyet ve kaza önleme gibi iste nilen gereksinimleri karşılayacak şekilde tasarlama becerisi**				x	

	c1	**Bildirilen ihtiyacların saptanması, işlevsel gereklerin ve kısıtlamaların belirlenmesi**			x	
		PC.c1	Problemin etki alanı tanımlanır ve arzu edilen ihtiyaçlara dayanarak gereksinimler belirlenir			
		PC.c2	Kısıtlamaları ve gereklilikleri kar şılayan uygun yöntemler seçilir	x		
	c2	**Bir tasarımın geliştirilmesi**			x	
		PC.c3	Uygun tasarım yöntemleri uygulanır	x		
		PC.c4	Yazılım sistemi, bileşeni ya da yöntemi tasarlanır	x		
		PC.c5	Donanım sistemi, bileşeni ya da yöntemi tasarlanır			x
		PC.c6	Uygun araçlarla tasarımın bütünü sunulur			
	c3	**Tasarımın gerçeklenmesi**		x		
		PC.c7	Tasarıma dayanan bir çözüm/prototip geli ştirilir		x	
	c4	**Geliştirilen çözümün testi ve do ğrulanması**			x	
		PC.c8	Test alt bileşenleri ve stratejileri tanımlanır	x		
		PC.c9	Geliştirilen çözümde hata ayıklaması yapılır ve tespit e dilen hatalar düzeltilir	x		
d	**Mevcut bir yapıyı veya sistemi eleştirel yaklaşımla gözleme, irdeleme ve sonuçta düzeltme ve iyile ştirme becerisi**				x	
	PC.d1	Mevcut bir yazılım ya da donanım sistemi i şlevselliğini incelemek için gözlemlenir				x
	PC.d2	Farklı olası durumları kapsayan iyi seçilmi ş girişler için çıkı şlar incelenir				x
	PC.d3	Bir sistemin kusurları bulunur ve düzeltilir				x
	PC.d4	Bir sistem gereksinimlere göre iyile ştirilir				x
e	**Birden çok disiplinden olu şan bir takım çalı şması yürütebilme becerisi**					x
	PC.e1	Uzun vadeli bir grup projesi ya da çok disiplinli b ir proje ekibine etkin bir takım üyesi olarak katılınır				
	PC.e2	Takımda sorumluluklar alınır ve yerine getirilir				
	PC.e3	Fikirlerin geliştirilmesinde yer alınır				
	PC.e4	Diğerlerinden alınan geri bildirimler düzeltmelere/iyi leştirmelere dahil edilir				
f	**Mühendislik problemlerini belirleme, formüle etme ve çözme becerisi**					x
	PC.f1	Bir bilgisayar mühendisli ği problemi belirlenir				x
	PC.f2	Bir bilgisayar mühendisli ği problem formal bir şekilde tanımlanır				
	PC.f3	Bir bilgisayar mühendisli ği problemine çözüm geli ştirilir				x
g	**Mesleki ve etik sorumlulukları kavrama**					x
	PC.g1	Profesyonel mühendislik uygulamalarına klavuz luk eden etik kuralların farkındadır			x	
	PC.g2	Verilecek bir kararla ilgili etik konular belirlenir ve tanımlanır				x
	PC.g3	Uygulamadaki bir durum gerçekler ve mesleki etik ku ralları göz önüne alınarak de ğerlendirilir ve hakkında hüküm verilir				
h	**Etkin sözlü ve yazılı ileti şim kurabilme becerisi**			x		
	h1	**Etkin yazılı iletişim bilgisi, kavramları ve fikirleri**		x		
		PC.h1	Uygun bir format ve dilbilgisi kullanılarak bir belge hazırlanır ve alıntılar dahil olmak üzere disipline özel kurallar kullanılır	x		
	h2	**Etkin sözlü ileti şim bilgisi, kavramları ve fikirleri**				
		PC.h2	İyi organize edilmiş bir sözlü sunum planlanır, hazırlanır ve teslim ed ilir; istenildiği zaman da sunulur			
	h3	**Grafiksel iletişim bilgisi, kavramları ve fikirleri**		x		
		PC.h3	Sözlü ve yazılı sunumlarda profesyonel grafik sel ö ğeler kullanılır	x		
i	**Mühendislik çözümlerinin küresel, toplumsal ve çevr esel boyutlarda etkisini kavramak için gereken geni ş kapsamlı bir eğitime sahip olma**			x		
	PC.i1	Bir mühendislik çözümünün birçok türde olası e tkileri listelenir		x		
	PC.i2	Toplum yapısını anlamayla ilgili, toplum, kültür ve evrensel toplum gibi terimleri içeren anahtar kelimeler tanımlanır		x		
	PC.i3	Küresel bir problemin mühendislik yönünün ayı rdına varılır		x		
j	**Yaşam boyu ö ğrenme gereğini algılamış ve kendi kendine ö ğrenme yeteneğini kazanmış olma**				x	
	j1	**Neyin ö ğrenilmesi gerektiğiyle ilgili bir farkındalık gösterme**			x	

		PC.j1	Gerçek bir projede neyin ö ğrenilmesi gerektiği belirlenir		x	
	j2	**Yaşam boyu ö ğrenme yeteneği**				
		PC.j2	Ö ğrenme planı gerçek bir projede ve/veya ba ğımsız bir ö ğrenme fırsatında uygulanır			
		PC.j3	Seminerlere ve staj aktivitelerine katılınır			
k	**Güncel/Ça ğdaş konulara ilişkin bilgi sahibi olma**			x		
		PC.k1	Potansiyel olarak doğaya etkileri olan mühendislik problemleri belirleni r			
		PC.k2	Temel sosyo-ekonomik konular listelenir ve tanımlanır	x		
		PC.k3	Ulusal ya da uluslararası seviyedeki temel politik konular listelenir ve tanımlanır	x		
l	**Mühendislik uygulamaları için gerekli teknikleri, y etenekleri ve modern mühendislik araç ve gereçlerin i kullanabilme becerisi**					x
		PC.l1	Mühendislik teknikleri, yetenekleri ve donanımları bir mühendislik sisteminin performansını gözlemlemek ve/veya bir mühendislik tasarımı yaratm ak için kullanılır		x	
		PC.l2	Mühendislik teknikleri, yetenekleri ve donanı mları karar verme için bilgi çıkarımında kullanılır			x
		PC.l3	Özel bir mühendislik görevi için uygun teknik ler ve donanımlar seçilir			x
m	**Değişen koşullara uyum sağlama yeteneği**					x
		PC.m1	Yeni araçlara ve yöntemlere uyum sa ğlanır			x
		PC.m2	Bir çalı şma grubunda farklı takım rolleri uygulanır			
		PC.m3	Gelişmekte olan alanların ayırdında olunur ve bunlara uyum sağlanır		x	

Relationship between the Course and Computer Engineering Curriculum

(1: "Little", 2: "Partial", 3: "Full", Leave blank if your answer is "None")

Computer Engineering Department Program Outcomes and Performance Criteria				**Level of Contribution**		
				1	**2**	**3**
a	**an ability to apply knowledge of mathematics, science, and engineering to the field of computer engineering**				X	
	a1	**Acquiring knowledge of mathematics, science and engineering**			X	
		PC.a1	answers questions on mathematics			
		PC.a2	answers questions on science and engineering		X	
	a2	**Applying knowledge of mathematics**				X
		PC.a3	applies mathematical principles to obtain analytical or numerical solutions to computer engineering problems			X
		PC.a4	chooses appropriate mathematical methods/approaches for a given problem			X
	a3	**Applying knowledge of science and engineering fundamentals**			X	
		PC.a5	applies science and engineering principles to model and solve computer engineering problems		X	
b	**an ability to design and conduct experiments, as well as to analyze and interpret data**					
	b1	**Designing experiments**				
		PC.b1	selects variables, appropriate equipment, test apparatus, model, etc			
		PC.b2	chooses the effective measure(s) by which the outcome or the alternative will be evaluated			
	b2	**Conducting experiments**				
		PC.b3	uses appropriate measurement techniques to collect data			
		PC.b4	documents collection procedures so that the experiment may be repeated			
	b3	**Analyzing data**				
		PC.b5	selects and uses appropriate tools (i.e., statistical and graphical) to analyze data			
	b4	**Interpreting data**				
		PC.b6	interprets results with respect to the original hypothesis			
c	**an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability**				X	
	c1	**Identifying stated needs and determining functional requirements and limitations**			X	
		PC.c1	describes scope of the problem and specifies the requirements based on the desired needs	X		
		PC.c2	selects appropriate methods satisfying the constraints and the requirements		X	
	c2	**Developing a design**		X		
		PC.c3	applies appropriate design methods	X		
		PC.c4	designs a software system, component or process			X
		PC.c5	designs a hardware system, component or process			
		PC.c6	presents the complete design with appropriate tools	X		
	c3	**Implementing the design**			X	
		PC.c7	develops a solution/prototype based on the design		X	
	c4	**Testing and validating the developed solution**		X		
		PC.c8	describes test cases and strategies	X		

		PC.c9	debugs the developed solution and corrects detected errors		X	
d	**an ability to observe and examine an existing structure or system in a criticizing attitude and finally correct or enhance it**					X
		PC.d1	observes an existing hardware/software system to analyze its functionality			X
		PC.d2	analyzes outputs given certain well-chosen inputs that cover different possible cases			X
		PC.d3	finds and corrects defects of a system			X
		PC.d4	enhances a system according to the requirements			X
e	**an ability to function on multi-disciplinary teams**					
		PC.e1	participates effectively as a team member in a long-term group/multi-disciplinary project team			
		PC.e2	takes and fulfills responsibilities in the team			
		PC.e3	participates in the development of ideas			
		PC.e4	incorporates feedback from others into revisions/improvements			
f	**an ability to identify, formulate, and solve engineering problems**					X
		PC.f1	identifies a computer engineering problem			X
		PC.f2	formally describes constituents of a computer engineering problem			
		PC.f3	develops a solution for a computer engineering problem			X
g	**an understanding of professional and ethical responsibility**					X
		PC.g1	is aware of the code of ethics that guide the professional practice of engineering		X	
		PC.g2	identifies and defines ethical issues concerning a decision			X
		PC.g3	evaluates and judges a situation in practice, using facts and a professional code of ethics			
h	**an ability to communicate effectively**			X		
	h1	**Written communication of information, concepts, and ideas effectively**		X		
		PC.h1	writes a document using an appropriate format and grammar and uses discipline-specific conventions including citations	X		
	h2	**Orally communicating information, concepts, and ideas effectively**				
		PC.h2	plans, prepares, and delivers a well-organized, logical oral presentation; explains when questioned			
	h3	**Graphically communicating information, concepts, and ideas**		X		
		PC.h3	uses professional graphics on written and oral presentations	X		
i	**the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental and societal context**			X		
		PC.i1	lists several types of impacts an engineering solution might have	X		
		PC.i2	defines key terms associated with understanding of a societal context including society, culture, and global society	X		
		PC.i3	recognizes the engineering aspects of a global problem	X		
j	**a recognition of the need for, and an ability to engage in life-long learning**				X	
	j1	**Demonstrating an awareness of what needs to be learned**			X	
		PC.j1	determines what needs to be learned in an actual project		X	
	j2	**Ability to engage in life-long learning**				
		PC.j2	applies the learning plan to an actual research project and/or independent learning opportunity			
		PC.j3	attends seminars and training activities			
k	**a knowledge of contemporary issues**			X		
		PC.k1	identifies engineering problems with potential environmental impact issues			
		PC.k2	lists and describes major socio-economic issues	X		
		PC.k3	lists and describes major political issues at national or international levels	X		
l	**an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice**					X
		PC.l1	uses engineering techniques, skills, and tools to monitor performance of an engineering system and/or create an engineering design		X	
		PC.l2	uses engineering techniques, skills, and tools to acquire information needed for decision-making			X
		PC.l3	selects appropriate techniques and tools for a specific engineering task			X
m	**an ability to adapt to changing conditions**					X
		PC.m1	adapts to new tools and approaches			X
		PC.m2	practices different team roles in a working group			
		PC.m3	is aware of emerging fields and adapts to them		X	

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
	27 Mayıs 2011	