

DERS TANIMLAMA FORMU

Dersin Kodu ve Adı	CENG468 E-İMZA VE AÇIK ANAHTAR ALTYAPISI (TEK.SEÇ.)
Dersin Yarıyılı	8
Dersin İçeriği	Ağ ortamında güvenilir iletişim sağlama ve güvenilir platform oluşturma
Ders Kitabı	Digital Signatures (Advances in Information Security), Jonathan Katz, Springer, 2010
Yardımcı Ders Kitapları	- Introduction to Public Key Infrastructures, Book by Alexander Wiesmaier, Evangelos Karatsiolis, and Johannes Buchmann, Springer, 2013 - Public Key Infrastructure: Building Trusted Applications and Web Services, Book by John R. Vacca, Auerbach Publications, 2014
Dersin Kredisi	6
Dersin Önkoşulları (Ders devam zorunlulukları, bu maddede belirtilmelidir)	-
Dersin Türü	Seçmeli
Öğretim Dili	İngilizce
Dersin Amaçları	Bilgi güvenliğinin temel ilkelerini, şifreleme algoritmalarını, ISO 27001 standartını öğretmek
Dersin Öğrenim Çıktıları	E-imza tanımı, bileşenleri, uygulamaları Güvenlik unsurları: veri bütünlüğü, kimlik doğrulama ve onaylama, inkâr edilmezlik, güvenlik gerekleri ve kullanılan yaklaşımlar Bilgisayar ve iletişim güvenliği Standartlar ISO 27001 Sayısal İmza Algoritmaları Anahtarlar Özetleme Algoritmaları Açık anahtar altyapısı ve bileşenleri. E-İmza Kanunu ve uygulamaları.
Dersin Veriliş Biçimi	Bu ders sadece yüz yüze eğitim şeklinde yürütülmektedir.
Dersin Haftalık Dağılımı	1) E-imza tanımı, bileşenleri, uygulamaları 2) Güvenlik unsurları, Veri bütünlüğü 3) Kimlik doğrulama ve onaylama 4) İnkâr edilmezlik 5) Güvenlik gerekleri ve kullanılan yaklaşımlar 6) Bilgisayar ve iletişim güvenliği 7) Standartlar, ISO 27001 8) Sayısal İmza Algoritmaları 9) Anahtarlar 10) Özetleme Algoritmaları 11) Açık anahtar altyapısı ve bileşenleri 12) E-imza yazılım ve donanımları 13) Açık anahtar altyapısı ve donanımları 14) E-İmza Kanunu, E-imza uygulamaları
Eğitim ve Öğretim Faaliyetleri (Bunlar örneklerdir. Lütfen dersinizde kullandığımız faaliyetleri doldurunuz.)	Haftalık teorik ders saati :3 Okuma Faaliyetleri İnternette tarama, kütüphane çalışması Ara sınav ve ara sınava hazırlık Final sınavı ve final sınavına hazırlık

Değerlendirme Ölçütleri		Sayısı	Toplam Katkısı (%)	
	Ara sınav	1	30	
	Ödev	5	30	
	Uygulama			
	Projeler			
	Pratik			
	Kısa Sınav			
	Dönem içi Çalışmaların Yıl İçi Başarıya Oranı (%)		60	
	Finalin Başarıya Oranı (%)		40	

Dersin İş Yüğü	Etkinlik	Toplam Hafta Sayısı	Süre (Haftalık Saat)	Dönem sonu Toplam İş Yüğü
	Haftalık teorik ders saati	14	3	42
	Haftalık uygulamalı ders saati			
	Okuma Faaliyetleri	12	4	48
	İnternette tarama, kütüphane çalışması	10	3	30
	Materyal tasarlama, uygulama			
	Rapor hazırlama			
	Sunu hazırlama			
	Sunum			
	Ara sınav ve ara sınava hazırlık	1	15	15
	Final sınavı ve final sınavına hazırlık	1	15	15
	Diğer			
	Toplam iş yüğü:			150
	Toplam iş yüğü / 25:			6
	Dersin AKTS kredisi:			6

Ders Çıktıları ile Program Çıktıları Arasındaki Katkı Düzeyi	No	Program Çıktıları	1	2	3	4	5
	1	Matematik, fen bilimleri ve bilgisayar mühendisliği konularında yeterli bilgi birikimi; bu alanlardaki kuramsal ve uygulamalı bilgileri mühendislik problemlerini modelleme ve çözüme için uygulayabilme becerisi					X
	2	Karmaşık mühendislik problemlerini saptama, tanımlama, formüle etme ve çözüme becerisi; bu amaçla uygun analiz ve modelleme yöntemlerini seçme ve uygulama becerisi				X	
	3	Karmaşık bir sistemi, süreci, cihazı, yazılımı, algoritmayı veya ürünü gerçekçi kısıtlar ve koşullar altında, belirli gereksinimleri karşılayacak şekilde tasarlama becerisi; bu amaçla güncel tasarım yöntemlerini uygulama becerisi			X		
	4	Mühendislik uygulamaları için gerekli olan modern teknik ve araçları seçme, geliştirme ve kullanma becerisi; bilişim teknolojilerini ve uygulamalarını etkin bir şekilde kullanma becerisi					X

	5	Mühendislik problemlerinin çözümü ve sonuçlarının analiz edilmesi için sistem veya deney tasarlama, gerçekleştirme, veri toplama ve yorumlama becerisi			X			
	6	Disiplin içi ve disiplinler arası takımlarda veya bireysel olarak etkin biçimde çalışabilme becerisi					X	
	7	Etkin rapor hazırlama, raporları değerlendirme ve yorumlama becerisi					X	
	8	Türkçe ve İngilizce sözlü ve yazılı etkin iletişim kurma, sunum yapma becerisi			X			
	9	Yaşam boyu öğrenmenin gerekliliği bilinci; bilgiye erişebilme, bilim ve teknolojiadaki gelişmeleri izleme ve kendini sürekli yenileme becerisi				X		
	10	Mesleki ve etik sorumluluk bilincine sahip olma ve etik ilkelerine uygun davranma becerisi					X	
	11	Proje yönetimi, risk yönetimi ve değişiklik yönetimi gibi konularda bilgi sahibi olma ve uygulama becerisi				X		
	12	Girişimcilik ve yenilikçilik konularında farkındalığa sahip olma ve sürdürülebilir sistemler oluşturabilme becerisi				X		
	13	Mühendislik uygulamalarının sağlık, çevre ve güvenlik üzerindeki etkilerini bilerek çağın sorunlarına toplumsal ve evrensel çözüm üretebilme becerisi		X				
	14	Mühendislik çözümlerinin hukuki sonuçları konusunda farkındalık sahibi olma		X				
	15	Yazılım geliştirme süreçleri ve dokümantasyon kuralları hakkında bilgi sahibi olma ve uygulama becerisi				X		
	16	Mühendislik uygulamalarında kullanılan standartlar hakkında bilgi sahibi olma					X	
	17	İş sağlığı ve güvenliği ile bilgi güvenliği ve mahremiyeti konularında farkındalık sahibi olma			X			
	Dersi Verecek Öğretim Eleman(lar)ı ve İletişim Bilgileri	Prof. Dr. Şeref SAĞIROĞLU ss@gazi.edu.tr						