DERS TANIMLAMA FORMU	
Dersin Kodu ve Adı	BM475 KRİPTOGRAFİYE GİRİŞ (TEK.SEÇ.)
Dersin Yarıyılı	7
Dersin İçeriği	Kriptografi ve şifreleme sistemlerinin temel kavramları. Klasik şifreleme sistemleri ve sayılar teorisi. Simetrik ve asimetrik algoritmalar. Veri şifreleme standardı (DES), ileri şifreleme standardı (AES), anahtarlar, anahtar yönetimi ve açık anahtarlar. RSA algoritması. Özetleme algoritmaları. Kriptografik protokoller.
Ders Kitabı	D. R. Stinson, Cryptography: theory and practice, 3rd edition, CRC, 2005.
Yardımcı Ders Kitapları	Introduction to Modern Cryptography: Principles and Protocols, J. Katz, Y. Lindell, CRC, 2007. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Bruce Schneier, 1996.
Dersin Kredisi	6
Dersin Önkoşulları **(***Ders devam zorunlulukları, bu maddede belirtilmelidir***)**	Bu dersin önkoşulu ya da eş koşulu bulunmamaktadır.
Dersin Türü	Teknik Seçmeli
Öğretim Dili	Türkçe
Dersin Amaçları	Öğrencilerin kriptografi, şifreleme sistemleri ve algoritmaları öğrenmeleri hedeflenmektedir.
Dersin Öğrenim Çıktıları	1. Kriptolografik algoritmaları, teknikleri ve dayandıkları matematiği anlayabilmek 2. Kriptografik algoritmaları kullanabilmek 3. Uygun kriptografik algoritmayı seçebilmek 4. Anahtar altyapıları hakkında bilgi sahibi olmak
Dersin Veriliş Biçimi	Bu ders sınıf ortamında yüz yüze eğitim şeklinde yürütülür.
Dersin Haftalık Dağılımı	1. Hafta: Kriptografi sistemlerinin temel kavramları 2. Hafta: Klasik şifreleme sistemleri ve sayılar teorisi 3. Hafta: Simetrik ve asimetrik algoritmalar 4. Hafta: Simetrik ve asimetrik algoritmalar 5. Hafta: Veri şifreleme standardı (DES) 6. Hafta: İleri şifreleme standardı (AES) 7. Hafta: Anahtarlar 8. Hafta: Anahtar yönetimi ve açık anahtarlar 9. Hafta: RSA algoritması 10. Hafta: RSA algoritması 11. Hafta: Özetleme algoritmaları 12. Hafta: Özetleme algoritmaları 13. Hafta: Kriptografik protokoller 14. Hafta: Kriptografik protokoller
Eğitim ve Öğretim Faaliyetleri *(Bunlar örneklerdir. Lütfen dersinizde kullandığınız faaliyetleri doldurunuz.)*	Haftalık teorik ders saati : 3 Okuma Faaliyetleri İnternetten tarama, kütüphane çalışması Materyal tasarlama, uygulama Ara sınav ve ara sınava hazırlık Final sınavı ve final sınavına hazırlık

	Sayısı	**Toplam Katkısı (%)**
Ara sınav	1	30
Ödev	2	30
Uygulama	0	
Projeler	0	

Değerlendirme Ölçütleri

Pratik	0	
Kısa Sınav	0	
Dönemiçi Çalışmaların Yıl İçi Başarıya Oranı (%)		60
Finalin Başarıya Oranı (%)		40
Devam Durumu		

Dersin İş Yükü

Etkinlik	Toplam Hafta Sayısı	Süre (Haftalık Saat)	Dönem Sonu Toplam İş Yükü
Haftalık teorik ders saati	14	3	42
Haftalık uygulamalı ders saati			0
Okuma Faaliyetleri	14	2	28
İnternetten tarama, kütüphane çalışması	12	2	24
Materyal tasarlama, uygulama	2	8	16
Rapor hazırlama			0
Sunu hazırlama			0
Sunum			0
Ara sınav ve ara sınava hazırlık	1	15	15
Final sınavı ve final sınavına hazırlık	1	20	20
Diğer			0
Toplam iş yükü			145
Toplam iş yükü/ 25			5.8
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 çözme için uygulayabilme becerisi			X		
2	Karmaşık mühendislik problemlerini saptama, tanımlama, formüle etme ve çözme 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 teknolojideki 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		Öğr.Gör.Dr Muhammet Ünal muhunal@gazi.edu.tr					