Ek 8. Ders Tanımlama Formu ***(Değişik: Gazi Üniversitesi Senatosunun 20/05/2021 tarihli ve 10 sayılı toplantısı, 2021/127 sayılı karar)***

DERS TANIMLAMA FORMU	
Dersin Kodu ve Adı	BM475 KRİPTOGRAFİYE GİRİŞ (TEK.SEÇ.)
Dersin Yarıyılı	7
Dersin Katalog Tanımı (*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.
Temel 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 (*AKTS*)	6
Dersin Önkoşulları (*Ders devam zorunlulukları, bu maddede belirtilmelidir.*)	Bu dersin önkoşulu ya da eş koşulu bulunmamaktadır.
Dersin Türü	Teknik Seçmeli
Dersin Öğretim Dili	Türkçe
Dersin Amacı ve Hedefi	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 Anahtar altyapıları hakkında bilgi sahibi olmak
Dersin Veriliş Biçimi *(Yüz yüze, Uzaktan vb.)*	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
Öğretim Faaliyetleri *(Burada belirtilen faaliyetler için harcanan zaman krediyi belirleyecektir. Dikkatli doldurulması gerekmektedir.)*	Haftalık teorik ders saati : 3 Okuma faaliyetleri İnternetten tarama, kütüphane çalışması Materyal tasarlama, uygulama Ara sınav ve ara sınava hazırlık Yarıyıl sonu sınavı ve yarıyıl sonu sınavına hazırlık

Değerlendirme Ölçütleri
(Toplam katkı yüzdesi 100 olacak şekilde ayarlanmalıdır.)

	Sayısı	Katkısı (%)
Ara sınav	1	30
Ödev	2	30
Uygulama	0	
Projeler	0	
Pratik	0	
Kısa sınav	0	
Yarıyıl sonu sınavı	1	40
Toplam	4	100

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 ve sunum			0
Ara sınav ve ara sınava hazırlık	1	15	15
Final sınavı ve final sınavına hazırlık	1	20	20
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, temel mühendislik, bilgisayarla hesaplama ve bilgisayar mühendisliği disiplinine özgü konularda bilgi; bu bilgileri, karmaşık mühendislik problemlerinin çözümünde kullanabilme becerisi.				X	
2	Karmaşık mühendislik problemlerini, temel bilim, matematik ve mühendislik bilgilerini kullanarak ve ele alınan problemle ilgili BM Sürdürülebilir Kalkınma Amaçlarını gözeterek tanımlama, formüle etme ve analiz becerisi.					X
3	Karmaşık mühendislik problemlerine yaratıcı çözümler tasarlama becerisi; karmaşık sistemleri, süreçleri, cihazları, yazılımları, algoritmaları veya ürünleri gerçekçi kısıtları ve koşulları gözeterek, mevcut ve gelecekteki gereksinimleri karşılayacak biçimde tasarlama becerisi.					X
4	Karmaşık mühendislik problemlerinin analizi ve çözümüne yönelik, tahmin ve modelleme de dâhil olmak üzere, uygun teknikleri, kaynakları ve modern mühendislik ve bilişim araçlarını, sınırlamalarının da farkında olarak seçme, kullanma ve geliştirme becerisi.			X		
5	Karmaşık mühendislik problemlerinin veya bilgisayar mühendisliği alanındaki araştırma konularının incelenmesi için literatür			X		

		araştırması, deney tasarlama, deney yapma, veri toplama, sonuçları analiz etme ve yorumlama dahil, araştırma yöntemlerini kullanma becerisi.					
	6	Mühendislik uygulamaları ve bu uygulamalarda kullanılan standartların BM Sürdürülebilir Kalkınma Amaçları kapsamında, topluma, sağlık ve güvenliğe, ekonomiye, sürdürülebilirlik ve çevreye etkileri hakkında bilgi; mühendislik çözümlerinin bilgi güvenliği ve hukuk alanlarında doğurduğu sonuçlar konusunda farkındalık.					X
	7	Mühendislik meslek ilkelerine uygun davranma, etik sorumluluk hakkında bilgi; hiçbir konuda ayrımcılık yapmadan, tarafsız davranma ve çeşitliliği kapsayıcı olma konularında farkındalık.					
	8	Bireysel olarak ve disiplin içi ve çok disiplinli takımlarda (yüz yüze, uzaktan veya karma) takım üyesi veya lideri olarak etkin biçimde çalışabilme becerisi.					
	9	Hedef kitlenin çeşitli farklılıklarını (eğitim, dil, meslek gibi) dikkate alarak, teknik konularda Türkçe veya İngilizce sözlü, yazılı etkin iletişim kurma, rapor hazırlama, etkili sunum yapma ve yazılım dokümantasyon hazırlama becerisi.				X	
	10	Proje, risk ve değişiklik yönetimi ve ekonomik yapılabilirlik analizi gibi iş hayatındaki uygulamalar hakkında bilgi; girişimcilik ve yenilikçilik hakkında farkındalık.					
	11	Bağımsız ve sürekli öğrenebilme, yeni ve gelişmekte olan bilimsel uygulamalara ve teknolojilere uyum sağlayabilme ve teknolojik değişimlerle ilgili sorgulayıcı düşünebilmeyi kapsayan yaşam boyu öğrenme becerisi.				X	

Dersi Verecek Öğretim Eleman(lar)ı ve İletişim Bilgileri	Öğr.Gör.Dr Muhammet Ünal muhunal@gazi.edu.tr