

	MSÜ DENİZ HARP OKULU DEKANLIĞI BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜM BAŞKANLIĞI DERS TANITIM BİLGİLERİ	
---	--	---

Dersin Adı	Dersin Kodu	Sınıf / Dönem	Ders Saati (T+U+L)	Kredi	AKTS
Kriptoloji (Siber Güvenlik)	BİL920	4 / Güz veya Bahar	3+0+0	3	3

Dersin Dili	:	Türkçe
Dersin Seviyesi	:	Lisans, Seçmeli
Dersin Önkoşulu	:	BİL205 AYRIK MATEMATİK
Dersin Öğretim Elemanları	:	Bilgisayar Mühendisliği Öğretim Elemanı
Dersin Amacı	:	Bu derste, klasik ve modern kriptolama teknikleri ve bunları deşifre yöntemleri öğretilecektir. Güvenli şifreleme ve kriptolama tekniğinin yapısı öğretilecektir. Amaca uygun şifreleme yöntemleri, anahtar üretme ve bunları güvenli bir şekilde dağıtma yöntemleri gösterilecektir.
Dersin Öğrenme Çıktıları	:	Bu dersi başarı ile tamamlayabilen öğrenciler; 1. Bilgisayar güvenliğinin temellerini bilir. 2. Kriptoloji kavramlarını, klasik şifreleme yöntemlerini bilir. 3. Modern şifreleme yöntemlerini ve uygulamalarını bilir. 4. Sayısal imza, özet fonksiyonları prensiplerini ve kullanım alanlarını bilir. 5. Güvenli anahtar değişimi prensiplerini bilir.
Dersin İçeriği	:	Kriptoloji kavramları, simetrik şifreleme, açık anahtar şifreleme, kriptografik özet fonksiyonları, mesaj doğrulama, sayısal imzalar, güvenli anahtar değişimi ve dağıtımı, kimlik doğrulama mekanizmaları, protokolleri

Ders Kitabı	:					
		Cryptography and Network Security: Principles and Practise	William STALLING	Pearson Educ.	2016	
		Şifreleme ve Şifre Çözme Yöntemleri	Nuri URAL-Ömer ÖRENÇ	Pusula Yayıncılık	2019	
Diğer Kaynaklar	:					
		Computer System and Network Security	Gregory B. WHITE Eric A. FISCH Udo W. POOCH	CRC Press	1995	
		Network Security Essentials: Applications and Standards	William STALLING	Pearson Educ.	2017	
Ödevler ve Projeler	:	-				
Bilgisayar Kullanımı	:	Var				
Diğer Uygulamalar	:	Yok				
Başarı Değerlendirme Sistemi	:	Faaliyetler		Taban Notu	Adedi	Değerlendirmedeki Katsayısı (%)
		Ara Sınav		50	1	%30
		Yarıyl Değerlendirme	Kısa Sınavlar	50	-	%10
			Ödevler	50	2	
			Projeler	50	-	
			Dönem Ödevi / Projesi	50	1	
			Laboratuvar Uygulaması	50	-	
			Diğer Uygulamalar	50	-	
			Bitirme Sınavı		50	1
		Bütünleme Sınavı / NYS		50	1	%100
		Çift Ders Sınavı		50	1	%100

PROGRAM ÇIKTILARININ DERSİN ÖĞRENME ÇIKTILARI İLE İLİŞKİSİ

Katkı Düzeyi	1	2	3	4	5
	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek

KRİPTOLOJİ

KRİPTOLOJİ															
		Program Çıktıları													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
Dersin Öğrenme Çıktıları	1	3	4	4	5	3	2	4	4	4	3	2	1	1	1
	2	4	4	4	5	3	2	3	2	3	3	2	1	1	1
	3	5	4	4	5	5	2	3	4	3	3	2	1	1	1
	4	5	4	4	5	5	2	3	3	2	2	2	1	1	1
	5	5	4	4	5	5	2	3	3	2	2	2	1	1	1

HAFTALIK KONULAR	
Hafta	Konular
1	Bilgisayar Sistemleri Güvenliğine Giriş
2	Şifreleme Teknikleri
3	Klasik Şifreleme
4	Gelişmiş Simetrik Şifreleme
5	İleri Kriptolama Standardı (AES)
6	Sonlu Alanlar
7	Sayılar Teoremi
8	ARA SINAV
9	Açık Anahtar Şifreleme ve RSA Algoritması
10	Anahtar Yönetimi
11	Mesaj Kimlik Denetimi ve Hash Fonksiyonları
12	Hash Algoritmaları
13	Sayısal İmza
14	Ayrık Logaritma Problemine Dayalı Açık Anahtarlı Kripto Sistemleri
15	Proje Sunumları

AKTS / İŞ YÜKÜ TABLOSU			
FAALİYETLER	SAYI	SÜRE	TOPLAM İŞ YÜKÜ
Teorik Ders	14	3	42
Uygulama	-	-	-
Sınıf Dışı Ders Çalışma Süresi	8	1	8
Ödev Hazırlama	2	2	4
Proje Hazırlama	1	4	4
Dönem Projesi Hazırlama	-	-	-
Dönem Projesi Sunumu	1	2	2
Ödev Sunumu	-	-	-
Proje Sunumu	-	-	-
Kısa Sınav	-	-	-
Ara Sınav	1	2	2
Ara Sınav İçin Bireysel Çalışma	1	10	10
Bitirme Sınavı	1	2	2
Bitirme Sınavı İçin Bireysel Çalışma	1	16	16
TOPLAM İŞ YÜKÜ	90 Saat		
DERSİN AKTS KREDİSİ	Toplam İş Yüğü / 30 = 90 / 30 =3 AKTS		

Son Güncelleme Tarihi	:	20.03.2024
Güncelleyen Kişi	:	Elif BOZKAYA ARAS