Ders Bilgi Formu

Ders Adı	Kodu	Yerel Kredi	AKTS	Ders (saat/hafta)	Uygulama (saat/hafta)	Laboratuar (saat/hafta)
Şifrelemeye Giriş	MTM4532	3	6	3	0	0

Önkoşullar	Yok

Yarıyıl	Bahar

Dersin Dili	İngilizce, Türkçe
Dersin Seviyesi	Lisans Seviyesi
Ders Kategorisi	Temel Meslek Dersleri
Dersin Veriliş Şekli	Yüz yüze

Dersi Sunan Akademik Birim	Matematik Mühendisliği Bölümü
Dersin Koordinatörü	Serkan Onar
Dersi Veren(ler)	Serkan Onar
Asistan(lar)ı	

Dersin Amacı	Sayılar teorisi bilgilerinin güncel hayata uygulanabilmesi.
Dersin İçeriği	Sayılar Teorisinde Bazı Temel Kavramlar ,Çarpanlara Ayırmanın Uygulamaları, Bazı Temel Şifreleme Yöntemleri, Matrislerle Şifreleme, Açık şifreleme Örnekleri.
Opsiyonel Program Bileşenleri	Yok

Ders Öğrenim Çıktıları

1	Şifreleme ve şifreleme analizi ile ilgili modern içeriği anlar.
2	Şifreleme için metodları kullanma ve analiz etme ve bu metodların uygulanabilirliği ve sınırları hakkında düşünür.
3	Bazı simetrik anahtarlı şifreleme sistemlerini ve açık anahtarlı şifreleme sistemlerinin bazı örneklerini uygular.
4	Modern simetrik ve açık anahtarlı şifreleme sistemlerinin felsefesini tasarlama ve detayları hakkında tartışabilir.
5	Öğrenciler sayılar teorisinin ve cebirin bazı uygulamalarını öğrenecektir.

Haftalık Konular ve İlgili Ön Hazırlık Çalışmaları

Hafta	Konular	Ön Hazırlık
1	Şifrelemeye Giriş, Tarihçe-Güdüleme	Ders kitabı 1
2	Sayılar Teorisinde Bazı Temel Kavramlar	Ders kitabı 1
3	Cebir Adımlarında Zaman Hesaplaması	Ders kitabı 1
4	Bölünebilme ve Öklit Algoritması	Ders kitabı 1
5	Kongrüanslar	Ders kitabı 1
6	Çarpanlara Ayırmanın Uygulamaları	Ders kitabı 1
7	Sonlu Cisimler ve Kuadratik Kalanlar	Ders kitabı 1
8	Ara Sınav 1	Ders kitabı 1

9	Sonlu Cisimler ve Kuadratik Kalanlar	Ders kitabı 1
10	Kuadratik Kalanlar	Ders kitabı 1
11	Bazı Temel Şifreleme Yöntemleri	Ders kitabı 1
12	Matrislerle Şifreleme	Ders kitabı 1
13	Açık şifreleme	Ders kitabı 1
14	RSA, Ayrık Logaritmalar, Knapsack	Ders kitabı 1
15	Final	Ders kitabı 1

Değerlendirme Sistemi

Etkinlikler	Sayı	Katkı Payı
Devam/Katılım		
Laboratuar		
Uygulama		
Arazi Çalışması		
Derse Özgü Staj		
Küçük Sınavlar/Stüdyo Kritiği		
Ödev		
Sunum/Jüri		
Projeler	1	30
Seminer/Workshop		
Ara Sınavlar	1	30
Final	1	40
Dönem İçi Çalışmaların Başarı Notuna Katkısı		60
Final Sınavının Başarı Notuna Katkısı		40
TOPLAM		100

AKTS İşyükü Tablosu

Etkinlikler	Sayı	Süresi (Saat)	Toplam İşyükü
Ders Saati	13	3	39
Laboratuar			
Uygulama			
Arazi Çalışması			
Sınıf Dışı Ders Çalışması	13	6	78
Derse Özgü Staj			
Ödev			0
Küçük Sınavlar/Stüdyo Kritiği			
Projeler	1	20	20
Sunum / Seminer			
Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi)	1	13	13
Final (Sınav Süresi + Sınav Hazırlık Süresi)	1	15	15

Toplam İşyükü	165
Toplam İşyükü / 30(s)	5.50
AKTS Kredisi	6

Diğer Notlar	Yok