Ders Bilgi Formu

Ders Adı	Kodu	Yerel Kredi	AKTS	Ders (saat/hafta)	Uygulama (saat/hafta)	Laboratuar (saat/hafta)
Şifreleme	MAT3557	3	5	3	0	0

Önkoşullar	Yok

Yarıyıl	Güz, Bahar

Dersin Dili	İngilizce, Türkçe
Dersin Seviyesi	Lisans Seviyesi
Ders Kategorisi	Uzmanlık/Alan Dersleri
Dersin Veriliş Şekli	Yüz yüze

Dersi Sunan Akademik Birim	Matematik Bölümü
Dersin Koordinatörü	Emre Kolotoğlu
Dersi Veren(ler)	Emre Kolotoğlu, Mustafa Sarı
Asistan(lar)ı	

Dersin Amacı	Sayılar teorisi bilgilerinin şifreleme bilimindeki uygulamalarını vermek.
Dersin İçeriği	Sayılar Teorisinde Bazı Temel Kavramlar, Kongrüanslar ve Çarpanlara Ayırma Uygulamaları, Bazı Temel Şifreleme Yöntemleri, Açık Anahtarlı Şifreleme, RSA, Ayrık Logaritma, Kuadratik Kalanlar, Sahte Asallar
Opsiyonel Program Bileşenleri	Yok

Ders Öğrenim Çıktıları

1	Öğrenciler sayılar teorisinin bazı uygulamalarını öğrenecektir.
2	Öğrenciler cebirin bazı uygulamalarını öğrenecektir.
3	Öğrenciler şifrelemenin temellerini öğrenecektir.
4	Öğrenciler bazı şifreleme metodlarını öğrenecektir.
5	Öğrenciler matematikte birçok konunun şifrelemede kullanıldığı öğrenecekler.

Haftalık Konular ve İlgili Ön Hazırlık Çalışmaları

Hafta	Konular	Ön Hazırlık
1	Şifrelemeye giriş, Tarihçe, Güdüleme	Ders Kitabı (Bölüm 1)
2	Cebir adımlarında zaman hesaplaması	Ders Kitabı (Bölüm 1)
3	Bölünebilme ve Öklit algoritması	Ders Kitabı (Bölüm 1)
4	Kongrüanslar	Ders Kitabı (Bölüm 1)
5	Çarpanlara ayırma uygulamaları	Ders Kitabı (Bölüm 1)
6	Bazı basit şifreleme sistemleri	Ders Kitabı (Bölüm 3)
7	Matrislerle şifreleme	Ders Kitabı (Bölüm 3)
8	Midterm 1 / Practice or Review	
9	Açık anahtarlı şifreleme	Ders Kitabı (Bölüm 4)
10	RSA	Ders Kitabı (Bölüm 4)

11	Ayrık Logaritma	Ders Kitabı (Bölüm 4)
12	Ara Sınav 2 / Sırt çantası problemi	Ders Kitabı (Bölüm 4)
13	Kuadratik kalanlar	Ders Kitabı (Bölüm 2)
14	Sahte Asallar	Ders Kitabı (Bölüm 5)
15	Tekrar	
16	Final	

Değerlendirme Sistemi

Etkinlikler	Sayı	Katkı Payı
Devam/Katılım		
Laboratuar		
Uygulama		
Arazi Çalışması		
Derse Özgü Staj		
Küçük Sınavlar/Stüdyo Kritiği		
Ödev		
Sunum/Jüri		
Projeler		
Seminer/Workshop		
Ara Sınavlar	2	60
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	14	3	42
Laboratuar			
Uygulama			
Arazi Çalışması			
Sınıf Dışı Ders Çalışması	14	5	70
Derse Özgü Staj			
Ödev			
Küçük Sınavlar/Stüdyo Kritiği			
Projeler			
Sunum / Seminer			
Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi)	2	15	30
Final (Sınav Süresi + Sınav Hazırlık Süresi)	1	15	15
Toplam İşyükü			157

Toplam İşyükü / 30(s)	5.23
AKTS Kredisi	5

Diğer Notlar	Yok