



Ders Bilgi Formu

Ders Adı	Kodu	Yerel Kredi	AKTS	Ders (saat/hafta)	Uygulama (saat/hafta)	Laboratuvar (saat/hafta)
Kriptografi	MAT5131	3	7.5	3	0	0

Önkoşullar	Yok
------------	-----

Yarıyıl	Güz, Bahar
---------	------------

Dersin Dili	İngilizce, Türkçe
-------------	-------------------

Dersin Seviyesi	Yüksek 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)	
------------------	--

Asistan(lar)ı	
---------------	--

Dersin Amacı	Bu dersin amacı, kriptografinin temel kavramlarını vermek, gizli ve açık anahtarlı şifreleme sistemlerini öğrencilere tanıtmak ve daha ileri düzeyde araştırma yapmak isteyen öğrenciler için gerekli alt yapıyı oluşturmaktır
--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Dersin İçeriği	Temel kriptosistemler, temel sayılar teorisi, blok şifreleme algoritmaları: DES ve AES(Rijindeal), açık anahtarlı kriptografi: RSA ve ayrık logaritma, Diffie Hellman anahtar değişim protokolü, dijital imzalar ve kimlik doğrulama, sır paylaşımı.
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Opsiyonel Program Bileşenleri	Yok
-------------------------------	-----

Ders Öğrenim Çıktıları

1	Öğrenciler şifrelemenin tarihçesini ve temel şifreleme sistemlerini öğrenecektir.
2	Öğrenciler temel düzeyde cebir ve sayılar teorisi öğrenecektir.
3	Öğrenciler gizli anahtarlı (private-key) ve açık anahtarlı (public key) şifreleme sistemlerini öğrenecektir.
4	Öğrenciler günümüzde kullanılan bazı şifreleme sistemlerini öğrenecektir.
5	Öğrenciler kimlik doğrulama işlemlerinde kullanılan dijital imzaları tanıyacaktır.

Haftalık Konular ve İlgili Ön Hazırlık Çalışmaları

Hafta	Konular	Ön Hazırlık
1	Bazı Basit Kriptosistemler	Kitap 1 Bölüm 1
2	Kriptanaliz	Kitap 1 Bölüm 1
3	Shannon Teori	Kitap 1 Bölüm 2
4	Blok Şifrelemeler	Kitap 1 Bölüm 3
5	Şifreleme Standartları	Kitap 1 Bölüm 3
6	Kriptografik Sağlama Fonksiyonları	Kitap 1 Bölüm 4
7	Kriptografik Sağlama Fonksiyonları	Kitap 1 Bölüm 4
8	RSA Kriptosistemi	Kitap 1 Bölüm 5

9	Tamsayıları Çarpanlara Ayırma	Kitap 1 Bölüm 5
10	Tamsayıları Çarpanlara Ayırma	Kitap 1 Bölüm 5
11	RSA Üzerinde Ataklar	Kitap 1 Bölüm 5
12	Açık-Anahtarlı Şifreleme	Kitap 1 Bölüm 6
13	Ayrık Logaritmalar	Kitap 1 Bölüm 6
14	Dijital İmzalar	Kitap 1 Bölüm 7
15	Sır paylaşımı	

Değerlendirme Sistemi

Etkinlikler	Sayı	Katkı Payı
Devam/Katılım		
Laboratuvar		
Uygulama		
Arazi Çalışması		
Derse Özgü Staj		
Küçük Sınavlar/Stüdyo Kritiği		
Ödev	6	30
Sunum/Jüri		
Projeler		
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
Laboratuvar			
Uygulama			
Arazi Çalışması			
Sınıf Dışı Ders Çalışması	13	9	117
Derse Özgü Staj			
Ödev	6	5	30
Küçük Sınavlar/Stüdyo Kritiği			
Projeler			
Sunum / Seminer			
Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi)	1	15	15
Final (Sınav Süresi + Sınav Hazırlık Süresi)	1	20	20

Toplam İşyükü	221
Toplam İşyükü / 30(s)	7.37
AKTS Kredisi	7.5

Diğer Notlar	Yok
--------------	-----