

SAYILAR TEORİSİ VE KRİPTOLOJİ

1	Ders Adı:	SAYILAR TEORİSİ VE KRİPTOLOJİ
2	Ders Kodu:	ADB6143
3	Ders Türü:	Seçmeli
4	Ders Seviyesi	Doktora
5	Dersin Verildiği Yıl:	1
6	Dersin Verildiği Yarıyıl	1
7	Dersin AKTS Kredisi:	6.00
8	Teorik Ders Saati (saat/Hafta)	3.00
9	Uygulama Ders Saati(saat/Hafta)	0.00
10	Laboratuvar Ders Saati (saat/hafta) :	0
11	Dersin Önkoşulu:	Yok
12	Dersin Dili:	Türkçe
13	Dersin Veriliş Şekli:	Yüz yüze
14	Dersin Koordinatörü:	Prof. Dr. MUSA DEMİRCİ
15	Dersi Veren Diğer Öğretim Elemanları:	Prof. Dr. İsmail Naci Cangül, Prof. Dr. Gökhan SOYDAN, Doç. Dr. Sibel KOPARAL
16	Koordinatör İletişim Bilgileri:	mdemirci@uludag.edu.tr, 02242941759
17	Dersin WEB adresi:	
18	Dersin Amacı:	Bu dersin amacı öğrencinin kriptoloji alanındaki bilgisini sayılar kullanarak çeşitlendirmeyi ve yükseltmeyi sağlamaktır.
19	Dersin Mesleki Gelişime Katkısı:	Bir çok disiplinde kullanılan özel sayı dizilerini biliyor ve bunları diğer disiplinlere uygulayabilir olmak.
20	Dersin Öğrenme Kazanımları:	
	1	Sayı kümelerini bilir.
	2	Sayılar üzerindeki bağıntıları bilir
	3	Kriptoloji kavramını bilir
	4	Şifre oluşturma ve kırma bilgisine sahip olur.
	5	
	6	
	7	
	8	
	9	
	10	
21	Dersin İçeriği:	
Hafta	DERS İÇERİKLERİ	
	Teorik	Uygulama
1	Çarpanlara ayırma ve bölme algoritması	
2	Asal sayılar ve bölünebilme	
3	Sonlu cisimler ve ikinci dereceden kalanlar	
4	Sayıların basamak sayıları	
5	Çarpımsal fonksiyonlar, Bölünenlerin sayısı	
6	Lineer Diophant denklemleri	

7	Kriptografik kavramlar, basit kriptografik kaynaklar.	
8	Genel anahtar	
9	Şifreleme ve şifre çözme	
10	Sürekli fonksiyonlar metodu	
11	Kriptografik genel anahtar fikri	
12	RSA, Discrete log şifreleme yöntemleri	
13	Elipitik eğri kriptosistemleri	
14	Asal sayılar ile şifreleme	

22	Ders Kitabı, Referanslar ve/veya Diğer Kaynaklar:	[1] Neal Koblitz, A Course in Number Theory and Cryptography. Springer-Verlag, New York, 1998. [2] Thomas Koshy, Fibonacci and Lucas Numbers with Applications. A Wiley-Interscience Publication, 2001. [3] Titu Andreescu, Dorin Andrica, Number Theory. Birkhauser,2009.
----	---	---

23	Değerlendirme	
----	---------------	--

YARIYIL İÇİ ÇALIŞMALARI	SAYISI	KATKI YÜZDESİ
Ara Sınav	0	0.00
Kısa Sınav	0	0.00
Ödev	0	0.00
Yıl Sonu Sınavı	1	100.00
Toplam	1	100.00
Yıl içi çalışmalarının Başarıya Oranı		0.00
Finalin Başarıya Oranı		100.00
Toplam		100.00
Kullanılan Ölçme ve Değerlendirme Yaklaşımları		Düzey belirleyici değerlendirme (Yarıyıl sonu sınavı)

24	AKTS / İŞ YÜKÜ TABLOSU
----	-------------------------------

ETKİNLİK	SAYISI	Süresi (Saat)	Toplam İş Yüğü (Saat)
Teorik Dersler	14	3.00	42.00
Uygulamalı Dersler	0	0.00	0.00
Sınıf Dışı Ders Çalışma Süresi (Ön çalışma, pekiştirme)	14	3.00	42.00
Ödevler	0	0.00	0.00
Projeler	0	0.00	0.00
Arazi Çalışmaları	0	0.00	0.00
Arasınavlar	0	0.00	0.00
Diğer	0	0.00	0.00
Yarıyıl Sonu Sınavı	1	96.00	96.00
Toplam İş Yüğü			180.00
Toplam İş Yüğü / 30 saat			6.00
Dersin AKTS Kredisi			6.00

25	PROGRAM YETERLİLİKLERİ İLE DERS ÖĞRETİM KAZANIMLARI İLİŞKİSİ TABLOSU															
	PY1	PY2	PY3	PY4	PY5	PY6	PY7	PY8	PY9	PY10	PY11	PY12	PY13	PY14	PY15	PY16
ÖK1	4	4	3	5	0	0	0	0	0	0	0	0	0	0	0	0
ÖK2	4	3	4	5	0	0	0	0	0	0	0	0	0	0	0	0
ÖK3	5	4	3	4	0	0	0	0	0	0	0	0	0	0	0	0
ÖK4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ÖK: Öğrenme kazanımlar PY: Program yeterlilikleri																
Katkı Düzeyi:	1 çok düşük			2 Düşük			3 Orta			4 Yüksek			5 Çok Yüksek			