

KRİPTOLOJİ

1	Ders Adı:	KRİPTOLOJİ
2	Ders Kodu:	BLPS260
3	Ders Türü:	Seçmeli
4	Ders Seviyesi	Önlisans
5	Dersin Verildiği Yıl:	2
6	Dersin Verildiği Yarıyıl	4
7	Dersin AKTS Kredisi:	3.00
8	Teorik Ders Saati (saat/Hafta)	2.00
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:	Öğr. Gör. Dr. ABDURRAHMAN DAYIOĞLU
15	Dersi Veren Diğer Öğretim Elemanları:	
16	Koordinatör İletişim Bilgileri:	dayioglu@uludag.edu.tr
17	Dersin WEB adresi:	
18	Dersin Amacı:	Kriptografi alanındaki temel kavram bilgisini kazandırmak.
19	Dersin Mesleki Gelişime Katkısı:	Öğrenciye, kriptografi alanındaki temel kavram bilgisini kazandırıp, meslek hayatında karşılaşılabileceği çeşitli durumlarda altyapısı hazır olur.
20	Dersin Öğrenme Kazanımları:	
	1	Temel kriptografi kavramlarını tanımlar.
	2	Kriptografinin temel matematiksel kavramlarını açıklar.
	3	Şifreleme algoritmaları konusunda teorik ve pratik bilgi ve deneyim kazanır.
	4	Açık anahtarlamalı kriptografik sistemlerin temel prensiplerini listeler.
	5	Kriptografinin genel güvenlikte oynadığı rolü anlar.
	6	Çeşitli gerçek dünya senaryoları için öğrendikleri içerisinden en iyi uygulama şifreleme şemalarını kullanma yeteneğini kazanır.
	7	Matematik ve Bilgisayar bilimleri bilgisini kullanarak yeni şifreleme ve kriptografi yöntemleri önerebilir.
	8	Şifreleme ve kriptografi yöntemlerini farklı güvenlik sistemlerinde uygulayabilir.
	9	Asallık testlerini kullanıp, çarpanlara ayırma yöntemlerini uygular ve temel kriptanaliz yöntemlerini tanımlar.
	10	
21	Dersin İçeriği:	
Hafta	DERS İÇERİKLERİ	
	Teorik	Uygulama
1	Dersin tanıtımı.	
2	Kriptolojinin temel hedefleri, Klasik kriptografi sistemlerine giriş.	

3	Klasik kriptografi sistemlerine detaylı bakış.	
4	Temel sayılar teorisine giriş.	
5	Sayılar ve polinomlar üzerine aritmetik işlemler ile blok şifreler.	
6	Sayılar ve polinomlar üzerine aritmetik işlemler ile akan şifreler.	
7	Açık Anahtar Kripto Sistemlerine giriş.	
8	Açık Anahtar Kripto Sistemleri	
9	Ayrık logaritma problemi	
10	Diffie-Hellman Anahtar Değişimi	
11	DSA, El-Gamal	
12	RSA	
13	Asallık testleri	
14	Çarpanlarına ayırma yöntemleri ile kriptanaliz yöntemleri	

22	Ders Kitabı, Referanslar ve/veya Diğer Kaynaklar:	Stinson, Douglas R. Cryptography: theory and practice. CRC press, 2005. Nigel Smart, Cryptography: An Introduction, Mcgraw-Hill Publication, 2004 William, Stallings, and William Stallings. Cryptography and Network Security, 6/E. Pearson Education India, 2014. Introduction to Modern Cryptography (2nd edition) by J. Katz and Y. Lindell. Kriptolojiye Giriş Ders Notları, Uygulamalı Matematik Enstitüsü, Odtü, 2004
----	---	---

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

YARIYIL İÇİ ÇALIŞMALARI	SAYISI	KATKI YÜZDESİ
Ara Sınav	1	40.00
Kısa Sınav	0	0.00
Ödev	0	0.00
Yıl Sonu Sınavı	1	60.00
Toplam	2	100.00
Yıl içi çalışmalarının Başarıya Oranı		40.00
Finalin Başarıya Oranı		60.00
Toplam		100.00
Kullanılan Ölçme ve Değerlendirme Yaklaşımları		Bağıl Değerlendirme

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

ETKİNLİK	SAYISI	Süresi (Saat)	Toplam İş Yüğü (Saat)
Teorik Dersler	14	2.00	28.00
Uygulamalı Dersler	0	0.00	0.00
Sınıf Dışı Ders Çalışma Süresi (Ön çalışma, pekiştirme)	14	2.00	28.00
Ödevler	14	2.00	28.00
Projeler	0	0.00	0.00
Arazi Çalışmaları	0	0.00	0.00
Arasınaylar	1	3.00	3.00
Diğer	0	0.00	0.00
Yarıyıl Sonu Sınavı	1	3.00	3.00
Toplam İş Yüğü			90.00
Toplam İş Yüğü / 30 saat			3.00
Dersin AKTS Kredisi			3.00

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	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK2	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK3	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK4	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK5	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK6	2	4	2	5	3	3	3	2	2	2	2	0	0	0	0	0
ÖK7	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK8	4	5	2	4	5	4	2	3	3	3	3	0	0	0	0	0
ÖK9	4	5	2	4	5	4	2	3	3	3	3	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							