KRİPTOGRAFİ

1	Ders Adi:	KRİPTOGRAFİ	
2	Ders Kodu:	BM5114	
3	Ders Türü:	Seçmeli	
4	Ders Seviyesi	Yüksek Lisans	
5	Dersin Verildiği Yıl:	1	
6	Dersin Verildiği Yarıyıl	2	
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:	Doç. Dr. Murtaza CİCİOĞLU	
15	Dersi Veren Diğer Öğretim Elemanları:	-	
16	Koordinatör İletişim Bilgileri:	murtazacicioglu at uludag.edu.tr	
17	Dersin WEB adresi:		
18	Dersin Amacı:	Klasik kriptografi: bazı basit kripto sistemleri, basit kripto sistemlerinin analizi. Shannon teorisi: olasılık teorisi, entropinin özellikleri, çarpım kriptosistemleri. Blok şifreleme algoritmaları: değiştirme-permütasyon ağları, lineer kriptanaliz, farksal kriptanaliz, veri şifreleme standardı (DES), ileri şifreleme standardı (AES), şifreleme modları. Kriptografik özet fonksiyonları: özet fonksiyonları ve veri bütünlüğü, özet fonksiyonlarının güvenliği, iteratif özet fonksiyonları, mesaj doğrulama kodları. RSA kriptosistemi: açık anahtarlı kriptosistemlerine giriş, sayı teorisi. Ayrık logaritma problemine dayalı açık anahtarlı kriptosistemleri: ElGamal kriptosistemi, sonlu cisimler, eliptik eğri kriptosistemi. Sayısal imza: sayısal imza sistemlerinin güvenlik gerekleri, ElGamal sayısal imza sistemi, DSA, ECDSA.	
19	Dersin Mesleki Gelişime Katkısı:	Güvenli iletişim teknikleri hakkında bilgi sahibi olması sağlanacaktır.	
20	Dersin Öğrenme Kazanımları:		
		1	Klasik kriptografi sistemlerinin hangi sebeple nasıl geliştiğini öğrenirler.
		2	Veri şifreleme standardı (DES) ve ileri şifrelem standardını (AES) gerçekleyebilirler.
		3	RSA kriptosistemini gerçekleyebilirler.
		4	ElGamal ve elliptik eğri kriptosistemlerini inceleyip gerçekleyebilirler.
		5	ElGamal sayısal imza sistemi, DSA ve ECDSA öğrenirler.
		6	
		7	
		8	

		9	
		10	
21	Dersin İçeriği:		
Hafta	**DERS İÇERİKLERİ**		
	Teorik		**Uygulama**
1	Klasik kriptografi: bazı basit kripto sistemleri, basit kripto sistemlerinin analizi.		
2	Klasik kriptografi: bazı basit kripto sistemleri, basit kripto sistemlerinin analizi.		
3	Shannon teorisi: olasılık teorisi, entropinin özellikleri, çarpım kriptosistemleri.		
4	Blok şifreleme algoritmaları: değiştirme-permütasyon ağları, lineer kriptanaliz, farksal kriptanaliz, veri şifreleme standardı (DES), ileri şifreleme standardı (AES), şifreleme modları.		
5	Blok şifreleme algoritmaları: değiştirme-permütasyon ağları, lineer kriptanaliz, farksal kriptanaliz, veri şifreleme standardı (DES), ileri şifreleme standardı (AES), şifreleme modları.		
6	Blok şifreleme algoritmaları: değiştirme-permütasyon ağları, lineer kriptanaliz, farksal kriptanaliz, veri şifreleme standardı (DES), ileri şifreleme standardı (AES), şifreleme modları.		
7	özet fonksiyonları: özet fonksiyonları ve veri bütünlüğü, özet fonksiyonlarının güvenliği, iteratif özet fonksiyonları, mesaj doğrulama kodları.		
8	özet fonksiyonları: özet fonksiyonları ve veri bütünlüğü, özet fonksiyonlarının güvenliği, iteratif özet fonksiyonları, mesaj doğrulama kodları.		
9	RSA kriptosistemi: açık anahtarlı kriptosistemlerine giriş, sayı teorisi.		
10	RSA kriptosistemi: açık anahtarlı kriptosistemlerine giriş, sayı teorisi.		
11	Ayrık logaritma problemine dayalı açık anahtarlı kriptosistemleri: ElGamal kriptosistemi, sonlu cisimler, eliptik eğri kriptosistemi.		
12	Ayrık logaritma problemine dayalı açık anahtarlı kriptosistemleri: ElGamal kriptosistemi, sonlu cisimler, eliptik eğri kriptosistemi.		
13	Sayısal imza: sayısal imza sistemlerinin güvenlik gerekleri, ElGamal sayısal imza sistemi, DSA, ECDSA.		
14	Sayısal imza: sayısal imza sistemlerinin güvenlik gerekleri, ElGamal sayısal imza sistemi, DSA, ECDSA.		
22	Ders Kitabı, Referanslar ve/veya Diğer Kaynaklar:		1) Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition by Bruce Schneier (Oct 18, 1996) Wiley; 2nd edition (October 18, 1996) 2) Christof Paar, Understanding Cryptography: A Textbook for Students and Practitioners", Springer; 1st Edition.2nd Printing edition (July 8, 2010). 3) Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, "Cryptography Engineering: Design Principles and Practical Applications" Wiley; 1 edition (March 15, 2010)

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		Yazılı sınav

24 AKTS / İŞ YÜKÜ TABLOSU

ETKİNLİK	SAYISI	Süresi (Saat)	Toplam İş Yükü (Saat)
Teorik Dersler	14	3.00	42.00
Uygulamalı Dersler	0	0.00	0.00
Sınıf Dışı Ders Çalışma Süresi (Ön çalışma, pekiştirme)	0	0.00	0.00
Ödevler	0	0.00	0.00
Projeler	0	0.00	0.00
Arazi Çalışmaları	0	0.00	0.00
Arasınavlar	1	60.00	60.00
Diğer	0	0.00	0.00
Yarıyıl Sonu Sınavı	1	80.00	80.00
Toplam İş Yükü			242.00
Toplam İş Yükü / 30 saat			6.07
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	2	4	4	3	5	3	0	0	0	0	0	0	0	0	0	0
ÖK2	3	4	4	5	3	5	0	0	0	0	0	0	0	0	0	0
ÖK3	3	4	1	3	3	4	0	0	0	0	0	0	0	0	0	0
ÖK4	3	4	2	3	3	1	0	0	0	0	0	0	0	0	0	0
ÖK5	3	4	1	5	4	4	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