

KRİPTOGRAFI

1	Ders Adı:	KRİPTOGRAFI
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:	Dr. Öğr. Üyesi CENGİZ TOĞAY
15	Dersi Veren Diğer Öğretim Elemanları:	-
16	Koordinatör İletişim Bilgileri:	Tel: 02242942796 ctogay@uludag.edu.tr
17	Dersin WEB adresi:	
18	Dersin Amacı:	Klasik kriptografi: bazı basit kriptosistemleri, basit kriptosistemlerinin 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. Ayırık 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 eliptik 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 kriptosistemleri, basit kriptosistemlerinin analizi.	
2	Klasik kriptografi: bazı basit kriptosistemleri, basit kriptosistemlerinin 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.	

[illegible]

ÖK: Öğrenme kazanımlar PY: Program yeterlilikleri

Katkı Düzeyi:	1 çok düşük	2 Düşük	3 Orta	4 Yüksek	5 Çok Yüksek
--------------------------	--------------------	----------------	---------------	-----------------	---------------------