DOKUZ EYLÜL ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ DEKANLIĞI

DERS/MODÜL/BLOK TANITIM FORMU

Dersi Veren Birim: Bilgisayar Mühendisliği			
Dersin Türkçe Adı: KRİPTOGRAFİYE GİRİŞ			**Dersin Orjinal Adı:** INTRODUCTION TO CRYPTOGRAPHY
Dersin Düzeyi:(Ön lisans, Lisans, Yüksek Lisans, Doktora) Lisans			**Dersin Kodu:** CME 4402
Dersin Öğretim Dili: İngilizce			**Formun Düzenleme / Yenilenme Tarihi:** 25/09/2012
Haftalık Ders Saati: 4			**Ders Koordinatörü (Ders girşinden sorumlu olan kişi):** YRD.DOÇENT GÖKHAN DALKILIÇ
Teori	**Uygulama**	**Laboratuvar**	**Dersin Ulusal Kredisi:** 3
2	2	0	**Dersin AKTS Kredisi:** 6

Dersi Alan Birimler	
Birim Adı	**Türü**
Bilgisayar Mühendisliği	Seçmeli

Dersin Öğretim Üyesi / Üyeleri

YRD.DOÇENT GÖKHAN

Dersin Amacı:

Bu dersin amacı öğrencilerin kriptografi ve algoritmaları öğrenmelerini sağlamaktır.

Dersin Öğrenme Çıktıları :

1 Kriptografik algoritmaları listeyebilme.

2 Güncel ve geleneksel kriptografik algoritmaları açıklayabilme.

3 Uygun kriptografik algoritmayı seçebilme.

4 Kriptografide kullanılan anahtarları yaratabilme.

5 Farklı kriptografik algoritmaları birlikte kullanabilme.

Öğrenme ve Öğretme Yöntemleri:

Sunum araçlarını kullanarak ders sınıfta anlatılacaktır. Programlama ödevleri ve projesi verilerek öğrencilerin sistemleri öğrenmesi beklenmektedir.

Değerlendirme Yöntemleri:

Adı	Kodu	Hesaplama Formülü
Vize	VZ	
Ödev	OD	
Final	FN	
BNS	BNS	VZ*020+D *030+FN * 050

Değerlendirme Yöntemlerine İlişkin Açıklamalar:

Değerlendirme Kriteri

1,2 ve 3. öğrenme çıktıları sınavlarda sorulacaktır.
4. ve 5. öğrenme çıktıları ödevler aracılığıyla desteklenecektir.

Ders İçin Önerilen Kaynaklar

Ders kitabı: Stallings, W., Cryptography and Network Security, Fifth Edition, Prentice Hall, New Jersey, 2011, ISBN: 0136097049
Referans kitabı: Cryptography: Theory and Practice, Stinson D.: ISBN: 1584882069, Publisher: Chapman & Hall

Derse İlişkin Politika ve Kurallar

Ders Öğretim Üyesi İletişim Bilgileri

eposta: dalkilic@cs.deu.edu.tr

Ders Öğretim Üyesi Görüşme Günleri ve Saatleri

Pazartesi 9:00-10:30

Dersin İçeriği

Hafta	Konular	Açıklama
1	Giriş	
2	Güvenlik Eğilimleri, Güvenlik Atakları, Servisler ve Mekanizmalar	
3	Klasik şifreleme teknikleri	
4	Blok şifreleme	
5	Veri Şifreleme Standardı (DES)	
6	Üçlü DES, Blok Şifreleme Mod İşlemleri, Akıcı Şifreleme Sistemleri	
7	Gelişmiş Şifreleme Standardı (AES)	
8	Vize	
9	Simetrik Şifreleme ile Gizlilik	
10	Anahtar dağıtımı	
11	Açık Anahtar şifreleme ve RSA	
12	Anahtar Yönetimi, Diğer Açık Anahtar Şifreleme Sistemleri	
13	Doğrulama Fonksiyonları	
14	Genel Tekrar	

AKTS Tablosu:

Derse İlişkin Etkinlikler	Sayısı	Süresi	Top.İşyükü
Ders İçi Etkinlikler			
Ders Anlatımı	13	2	26
Uygulama	14	2	28
Sınavlar			
Vize Sınavı	1	2	2
Final Sınavı	1	2	2
Ders Dışı Etkinlikler			
Haftalık Ders öncesi/sonrası hazırlıklar	13	2	26
Vize Sınavına Hazırlık	1	10	10
Final Sınavına Hazırlık	1	16	16
Ödev Hazırlama	4	8	32
Toplam İşyükü			142
Dersin AKTS Kredisi			6