DOKUZ EYLÜL ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DERS/MODÜL/BLOK TANITIM FORMU

Dersi Veren Birim: Fen Bilimleri Enstitüsü			
Dersin Türkçe Adı: Kriptosistemler ve Kriptografik Protokoller			**Dersin Orjinal Adı:** Cryptosystems and Cryptographic Protocols
Dersin Düzeyi:(Ön lisans, Lisans, Yüksek Lisans, Doktora) Lisansüstü			**Dersin Kodu:** CSE 6011
Dersin Öğretim Dili: İngilizce			**Formun Düzenleme / Yenilenme Tarihi:** 09/04/2013
Haftalık Ders Saati: 3			**Ders Koordinatörü (Ders girşinden sorumlu olan kişi):** YRD.DOÇENT GÖKHAN DALKILIÇ
Teori	**Uygulama**	**Laboratuvar**	**Dersin Ulusal Kredisi:** 3
3	0	0	**Dersin AKTS Kredisi:** 8

DOKUZ EYLÜL ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DERS/MODÜL/BLOK TANITIM FORMU

Dersi Alan Birimler	
Birim Adı	**Türü**
Bilgisayar Müh. Doktora	Seçmeli
Bilgisayar Müh. Yüksek Lisans	Seçmeli

DOKUZ EYLÜL ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DERS/MODÜL/BLOK TANITIM FORMU

Dersin Öğretim Üyesi / Üyeleri

YRD.DOÇENT GÖKHAN

Dersin Amacı:

Bu dersin amacı öğrencilerin iyi bilinen kriptosistemleri ve kriptografik protokolleri öğrenmelerini sağlamaktır.

Dersin Öğrenme Çıktıları :

1 İyi bilinen kriptosistemleri tarif edebilme

2 Kriptografik algoritmaları sınıflayabilme

3 Uygun kriptografik protokolü seçebilme

4 Uygun algoritmaları kullanabilme

5 Anahtarların önemini açıklayabilme

Öğrenme ve Öğretme Yöntemleri:

Sunum araçları ile ders sınıfta işlenecektir. Programlama ödevleri ve proje verilerek tüm öğrencilerin güvenlik sistemlerini öğrenmesi beklenmektedir.

Değerlendirme Yöntemleri:

Adı	Kodu	Hesaplama Formülü
Termpaper	TP	
Prsentation	PR	
Final	FN	
BNS	BNS	TP * 025 + PR * 025 + FN * 050

Değerlendirme Yöntemlerine İlişkin Açıklamalar:

Değerlendirme Kriteri

Ders İçin Önerilen Kaynaklar

Ana kaynak: Stallings, W., Cryptography and Network Security, Fifth Edition, Prentice Hall, New Jersey, 2011, ISBN: 0136097049
Yardımcı kaynak: Stinson, D.R., Cryptography Theory and Practice, CRC Press, 1995, ISBN 0-8493-8521-0
Referanslar: Dergi makaleleri

DOKUZ EYLÜL ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DERS/MODÜL/BLOK TANITIM FORMU

Derse İlişkin Politika ve Kurallar

Ders Öğretim Üyesi İletişim Bilgileri

Yrd. Doç. Dr. Gökhan DALKILIÇ
Dokuz Eylül Üniversitesi
Bilgisayar Mühendisliği Bölümü
Tınaztepe Yerleşkesi 35160 BUCA/İZMİR
Tel: (232) 301 74 01
E-Posta: dalkilic@cs.deu.edu.tr

Ders Öğretim Üyesi Görüşme Günleri ve Saatleri

Dersin İçeriği

Hafta	Konular	Açıklama
1	Giriş	
2	Klasik Kriptografi	
3	Shannon Teorisi	
4	Veri Şifreleme Standardı (DES)	
5	RSA Sistemi ve Çarpanlarına Ayırma	
6	Diğer Açık Anahtar Kriptosistemler	
7	Hash Fonksiyonları	
8	Anahtar Dağıtımı ve Yönetimi	
9	Tanımlama Şemaları	
10	Sanal Rastgele Sayı Üretimi	
11	Sayısal İmzalar ve Doğrulama Protokolleri	
12	Doğrulama Uygulamaları	
13	Hafif Doğrulama Fonksiyonları	
14	Elektronik Posta Güvenliği	

DERS/MODÜL/BLOK TANITIM FORMU

AKTS Tablosu:

Derse İlişkin Etkinlikler	Sayısı	Süresi	Top.İşyükü
Ders İçi Etkinlikler			
Ders anlatımı	15	3	45
Sınavlar			
Final Sınavı	1	2	2
Ders Dışı Etkinlikler			
Haftalık ders öncesi/sonrası hazırlıklar (ders materyalle	15	4	60
Final sınavına hazırlık	1	15	15
Ödev hazırlama	4	8	32
Sunum hazırlama	1	4	4
Diğer (araştırma, makale okuma, vb.)	2	15	30
Toplam İşyükü			188
Dersin AKTS Kredisi			8