



Dersi Veren Birim: Fen Bilimleri Enstitüsü			
Dersin Türkçe Adı: Güvenlik ve Gizlilik Mühendisliği		Dersin Orjinal Adı: Security and Privacy Engineering	
Dersin Düzeyi: (Ön lisans, Lisans, Yüksek Lisans, Doktora) Lisansüstü		Dersin Kodu: CSE 5065	
Dersin Öğretim Dili: İngilizce		Formun Düzenleme / Yenilenme Tarihi: 16/02/2013	
Haftalık Ders Saati: 3		Ders Koordinatörü (Ders girşinden sorumlu olan kiři): PROFESÖR SÜLEYMAN SEVİNÇ	
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

Bilgisayar Müh. Tezsiz Yüksek Lisans (İ.Ö)

Seçmeli

Bilgisayar Müh. Tezsiz Yüksek Lisans

Seçmeli



Dersin Öğretim Üyesi / Üyeleri

Dersin Amacı:

Dersin amacı öğrencilerde güvenli ve kişisel verilerin korunmasına saygılı bilgi sistemleri tasarımı konusunda bilgi ve beceri oluşturmaktır.

Dersin Öğrenme Çıktıları :

- 1 Sayılar teorisinin güvenlik problemlerine uygulayabilmek
- 2 Kişisel verilerin korunması prensiplerini tanımlayabilmek
- 3 Güvenlik ve kişisel verilerin korunması algoritmalarının doğruluğunun kanıtlayabilmek
- 4 Kişisel verilerin korunmasına saygılı ve güvenli sistemlerin tasarlayabilmek
- 5 Güvenlik ve kişisel verilerin korunmasına karşı riskleri tanımlayabilmek

Öğrenme ve Öğretme Yöntemleri:

Teorik dersler, ev ödevleri, bağımsız proje çalışmaları, problem kümeleri

Değerlendirme Yöntemleri:

Adı	Kodu	Hesaplama Formülü
Midterm	MD	
Assignment1	AS1	
Assignment2	AS2	
Final	FN	
BNS	BNS	$MD * 030 + AS1 + AS2/2 * 020 + FN * 050$

Değerlendirme Yöntemlerine İlişkin Açıklamalar:

Değerlendirme Kriteri

Ders İçin Önerilen Kaynaklar

Ders Kitapları:

Stallings, W., Network Security Essentials 4th Edition, Prentice Hall, New Jersey, 2010, ISBN 0137067925

Edited by G. Goos, J. Hartmanis and J. van Leeuwen, IT-Security And Privacy, Design and Use of Privacy-Enhancing Security Systems, Lecture Notes in Computer Science, Springer, 2001.



Yardımcı Kitap: Eynden, Charles, V. Elementary Number Theory, Mc Graw Hill, 2001.

Diğer Kitaplar: Schneier, Bruce. Applied Cryptography, John Wiley and Sons, 1996.
Anderson Ross J., Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Publishing, 2008, ISBN: 978-0-470-06852-6

Malzemeler: Ders notları, makaleler, problem kümeleri

Derse İlişkin Politika ve Kurallar

Ders Öğretim Üyesi İletişim Bilgileri

Prof.Dr. Suleyman Sevinc
Dokuz Eylul University
Department of Computer Engineering
Tinaztepe Campus 35160 BUCA/IZMIR
Tel: +90 (232) 301 74 01
e-mail: suleyman.sevinc@cs.deu.edu.tr

Ders Öğretim Üyesi Görüşme Günleri ve Saatleri

İlk derste duyurulacaktır

Dersin İçeriği

Hafta	Konular	Açıklama
1	Güvenlik ve Kişisel verilerin korunması kavramlarına giriş	
2	Sayılar Teorisi temelleri	
3	Asal sayılar ve asallık testleri	
4	Simetrik anahtarlı şifreleme, DES	
5	Discrete Logaritma, PKI, RSA	
6	Kimlik doğrulama, Hashing, Dijital İmza	
7	Güvenlik ve kişisel verilerin korunmasına karşı riskler ve tehditler	
8	Sır paylaşma algoritmaları	
9	Kişisel verilerin korunması ile ilgili algoritmalar	
10	Kişisel verilerin korunması : Hukuki prensipler ve bilgisayar gerçeklemeleri	



DOKUZ EYLÜL ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

DERS/MODÜL/BLOK TANITIM FORMU

- 11 Sistem düzeyinde tasarım
- 12 Elektronik oylama örneği
- 13 Sağlık verilerinin korunması, diğer örnekler
- 14 Gözden geçirme



AKTS Tablosu:

Derse İlişkin Etkinlikler	Sayısı	Süresi	Top.İşyükü
Ders İçi Etkinlikler			
Ders Anlatımı	39	1	39

Sınavlar	Sayısı	Süresi	Top.İşyükü
Final Sınavı	1	2	2
Vize Sınavı	2	2	4
Diğer Kısa Sınav	3	3	9

Ders Dışı Etkinlikler	Sayısı	Süresi	Top.İşyükü
Haftalık Ders öncesi/sonrası hazırlıklar	13	5	65
Vize Sınavına Hazırlık	2	10	20
Final Sınavına Hazırlık	1	15	15
Diğer Kısa Sınavlara Hazırlık	3	3	9
Ödev Hazırlama	4	4	16
Kitap Okuma	3	7	21
Toplam İşyükü			200
Dersin AKTS Kredisi			8