Öğretim Yılı: 2010-2011

DERS TANITIM FORMU

Dersin Kodu	CENG 471	**Dersin Adı**	Kriptografi		
Dönem	Güz /4. sınıf	**Kredisi**	**Teorik**	**Uygulama**	**ECTS**
			3	0	6
Program Adı	Bilgisayar Mühendisliği Lisans				
Dersin Tipi	Zorunlu [ ]	Seçmeli [ ]	Alan [x]	**Alan Adı**	Güvenlik

Ön Şartlar		**Dersin Dili**	İngilizce
Toplam Ders Saati	42 saat teorik		
Kişisel Çalışma (Teorik)	1 saat / hafta	**Kişisel Çalışma (Uygulama)**	1 saat / hafta
Ödevler, projeler, sunumlar vb. aktiviteler için önerilen toplam çalışma süresi			18 saat
Dersi Veren Öğretim Üyesi	Yrd. Doç. Dr. Serap Şahin		

Kısa Tanıtım

Kriptografinin tarihsel gelişimi, gereksinim duyulan güvenlik fonksiyonları ve bu fonksiyonların konvansiyonel, simetrik ve asimetrik kripto sistemler tarafından nasıl sağlandığı, zayıflıkları ve saldırı şekilleri öğrenilmektedir. Kripto sistemlerin güvenlik seviyelerini ve zayıflıklarını öğrencilerin anlayabilmesi için sayılar kuramı, soyut cebir gibi alanlardan gerekli matematik kuram ve yapılar konularla paralel olarak öğretilmektedir. Öğrenciler dönem ödevi olarak kriptografik araçların farklı alanlarda uygulamalarını inceleyerek, konu, ilgili problemler ve yanıtları hakkında bir rapor ve sunuş hazırlar, sınıfta sunar.

Dersin Hedefleri

DH1. Bilgi güvenliğinin önemi, güvenlik tehdit şekilleri ve güvenlik fonksiyonlarının bilinmesi.
DH2. Güvenlik fonksiyonlarının nasıl ve hangi kriptografik araçlarla sağlanıldığının öğrenilmesi.
DH3. Kriptografinin tarihsel gelişimi, simetrik ve asimetrik kriptografi
DH4. Kriptosistemlerin güvenlik seviyelerinin nasıl belirleneceğinin ve ilgili standartların bilinmesi.
DH5. Güvenlik gereksinimine göre kriptografik bir güvenlik çözümünü belirleme ve oluşturabilme kabiliyetinin elde edilmesi.
DH6. Günümüz bilişim ve iletişim teknolojilerinde kullanılan güvenlik çözümlerinin öğrenilmesi.

Dersin İşleniş Biçimi, Öğretme/Öğrenme Yöntemleri

Dersler haftada 3 saat sınıfta teorik şeklinde olmaktadır. Teorik derslerde konu anlatımı tahta ve sunum yardımıyla yapılmakta, soru-cevap bölümleri ve kısa sınavlar ile öğrenme seviyesi ve hızı test edilmektedir. Ders sürecinde öğrencilere kodlama ödevleri verilerek kuramsal konuları kavramaları sağlanmaktadır. Özellikle dönem sonunda raporlanan ve sunulan dönem ödevi öğrenilenlerin mesleki gelecek yaşamlarında pratik deneyim kazandıracak şekilde belirlenmektedir.

Ders Kitabı

- Wade Trappe & Lawrence Washington , Introduction to Cryptography with Coding Theory, Pearson, 2006, 0-13-198199-4

Yardımcı Kaynaklar

- Peter Gutman, Cryptographic Security Architecture, Springer, 2004, 0-387-95387-6
- Douglas R. Stinson, Cryptography, Theory and Practice, Chapman & Hall/CRC Press, 2002, 1-58488-206-9
- Bruce Schneider, Applied Cryptography, Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 1996, 0-471-12845-7

Kullanılan Materyal, Laboratuvar Malzemesi ve Yazılımlar

Windows İşletim Sisteminde, Visual C kod geliştirme platformunda, Windows APIs, GMP ve MIRACL gibi multiprecision kriptografik kod geliştirme kütüphaneleri.

Değerlendirme

Ara Sınavlar	%40	**Kısa Sınavlar**	-	**Dönem Sonu Sınavı**	-
Ödevler	%30	**Dönem Ödevi - Proje**	-	**Laboratuvar**	-
Rapor ve Sunum	%30	**Diğer**	-		

Haftalık Ders Planı

H1. Gizlilik, bütünlük ve kimlik denetimi ile ilgili temel tanımlar ve kriptografi tarihi.

H2. Bilgi kuramı ve Olasılık kuramı ile ilgili temel kavramlar.

H3. Monoalphabetical & Polyalphabetical yerine koyma yöntemi

H4. Transpositions-Permutations

H5. Blok şifreleme, DES-AES

H6. Simetrik anahtar yönetimi ve güvenlik mimarisi.

H7. Simetrik kriptosistem tasarım ve doğrulama.

H8. Sayılar kuramına giriş, kavramlar I

H9. Sayılar kuramına giriş, kavramlar II

H10. Faktorizasyon tabanlı kriptosistem: RSA

H11. Ayrık Logaritma problemi ve kriptosistemler: DHKE, ElGamal

H12. Elliptik Eğri Kriptosistem: ECC

H13. PKI – Açık Anahtar Altyapısı

H14. Kriptografik Protokol tasarımı FIPS 140-2/3

Dersin Hedefleri – Haftalık Ders Planı Matrisi (2: Katkısı var, 1: Katkısı kısmen var, 0: Katkısı yok)

	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10	H11	H12	H13	H14
DH1	2				1	1	2			2	2	2	1	2
DH2					2	2	2			2	2	2		1
DH3	2	2	2	2	2	2	1	1	1	2	2	2		
DH4						2							1	2
DH5														2
DH6					2					2	1	2	2	1
TOPL.	**4**	**2**	**2**	**2**	**7**	**7**	**5**	**1**	**1**	**8**	**7**	**8**	**4**	**8**

Dersin Hedefleri – Program Çıktıları Matrisi (2: Katkısı var, 1: Katkısı kısmen var, 0: Katkısı yok)

	PÇ1	PÇ2	PÇ3	PÇ4	PÇ5	PÇ6	PÇ7	PÇ8	PÇ9	PÇ10	PÇ11	PÇ12	PÇ13	PÇ14	PÇ15
DH1	1	2	1	1											
DH2	2	1	1												
DH3	1		1	2											
DH4	2	2	1	1											
DH5		2	2												
DH6		2	2												
TOPL.	**6**	**9**	**8**	**4**											