BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
DERS BİLGİ FORMU

Dersin Ayrıntıları				
Dersin Kodu	**Sınıfı**			**Yarıyılı**
INF047	4			Güz, Bahar
Dersin Adı	**T**	**U**	**L**	**AKTS**
Kodlama Teorisi ve Kriptoloji	2	0	2	6

Dersin Dili	Almanca					
Dersin Düzeyi	**Lisans**	**X**	**Yüksek Lisans**		**Doktora**	
Bölümü/Programı	Bilgisayar Mühendisliği					
Eğitim Türü	Yüzyüze ders anlatımı, grup çalışması, kişisel çalışma.					
Dersin Türü	**Zorunlu**		**Seçmeli**	**X**		
Dersin Amacı	Bu dersi başarı ile tamamlayan bir öğrenci aşağıdaki konularda kapsamlı bilgiye sahip olacaktır; - Temel kodlama teorisi (oran, ağırlık, mesafe, bir kodun mesafesi, sınırlar, hata düzeltme / algılama, eşlik üreten matris ve kontrol matrisini içeren lineer kodlar ve mesafeyi bulmak için ikincisinin nasıl kullanılacağı) - Hata tespit ve hata düzeltme teorisinde Hamming mesafesi ve bir kodun minimum mesafesini kavramlarının önemi - Doğrusal cebir, doğrusal kodlar teorisinde iyi etki için nasıl kullanılabilir. - En temel örneklerden modern açık anahtar sistemlerine kadar kriptografi - Açık anahtarlı şifreleme sistemlerinde kullanılan sayı teorik kavramları ve bunların pratik örneklerde nasıl uygulandığını göstermek					
Dersin İçeriği	- Hata düzeltme ve hata algılama kodları - Sayı Teorisi (Gruplar, Alanlar, Vektör Uzayları, Polinomlar) - Doğrusal kodlar - Tarihsel şifreler - Simetrik / Özel anahtarlı kripto - Asimetrik / Açık Anahtarlı kripto - Protokoller					
Ön Koşulları	Yok					
Dersin Koordinatörü	Dr. Öğr. Üyesi Canan Yıldız					
Dersi Verenler	Dr. Öğr. Üyesi Canan Yıldız					
Dersin Yardımcıları						
Dersin Staj Durumu	Yok					

Ders Kaynakları	
Ders Notu	- Hill, Raymond. A first course in coding theory. Oxford University Press, 1986. - Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2014.
Diğer Kaynaklar	- Trappe, Wade, and Lawrence C. Washington. "Introduction to Cryptography." (2007). - Koblitz, Neal. A course in number theory and cryptography. Vol. 114. Springer Science & Business Media, 1994.

Materyal Paylaşımı

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
DERS BİLGİ FORMU

Dokümanlar	-	
Ödevler	-	
Sınavlar	-	
Dersin Yapısı		
Matematik ve Temel Bilimler	50	%
Mühendislik Bilimleri		%
Mühendislik Tasarımı		%
Sosyal Bilimler		%
Eğitim Bilimleri		%
Fen Bilimleri		%
Sağlık Bilimleri		%
Alan Bilgisi	50	%

Değerlendirme Sistemi		
	Sayısı	**Katkı Oranı (%)**
Ara Sınav	1	40
Kısa Sınav		
Ödev	1	10
Devam		
Uygulama		
Proje		
Yarıyıl Sonu Sınavı	1	50
	Toplam	**100**

AKTS İş Yükü Dağılımı Tablosu			
	Sayısı	**Süresi**	**Toplam İş Yükü (Saat)**
Ders Süresi	14	2	28
Sınıf Dışı Ç. Süresi	1	66	66
Ödevler	10	4	40
Sunum/Seminer Hazırlama			
Ara Sınavlar	1	3	3
Uygulama	14	2	28
Laboratuvar			
Proje			
Yarıyıl Sonu Sınavı	1	3	3
		Toplam İş Yükü	**168**
		AKTS Kredisi (Toplam İş Yükü / 28)	**6**

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
DERS BİLGİ FORMU

Dersin Öğrenim Çıktıları	
1	Doğrusal kodlar kullanarak hata tespit ve hata düzeltme teorisinin altında yatan matematiksel fikirleri anlar.
2	Hata tespit ve hata düzeltme kodları teorisini uygular.
3	Kriptografi teorisinin altında yatan matematiksel fikirleri anlar.
4	Kriptografi teorisini uygular.
5	Kodlama teorisi ve kriptografide kanıtları açıklar ve oluşturur.
Ders Konuları	
1	Gürültülü Kanallar, Kodlama / Kod Çözme, İkili Simetrik Kanal, Maksimum Olabilirlik Kod Çözme, Hata Olasılıkları, Tekrar Kodları, Hamming Ağırlığı
2	Hamming Mesafesi, Blok Kodlar, Alfabeler, Hata Düzeltme, Hata Tespit, Genel Hamming Kodu, Ana Kodlama Teorisi Sorunu
3	Soyut Cebir alt dersinin başlangıcı. Tanıtılan Gruplar, Alanlar, Halkalar, Modüler Aritmetik.
4	Cebir Bölüm 2: Dihedral Gruplar, Permütasyon Grupları, Alt Gruplar, Vektör Uzayları, Sonlu Cisimler, Kosetler
5	Cebir Bölüm 3: Jeneratörler, Bazlar, Emirler, Fermat'ın Küçük Teoremi, Euler Fermat Teoremi, Legendre Teoremi, Altuzaylar.
6	Vektör Uzaylarından Doğrusal Kodlara. Jeneratör ve Parite Kontrol Matrisi Oluşturma
7	Golay kodları, çift kodlar, kod çözme doğrusal kodları.
8	Kriptoya giriş
9	Ara sınav
10	Hesaplamalı Güvenlik, Sözde Rastgele Jeneratörler, Ayrıştırılamazlık, PRG'den PKE'ye Akış ve Blok Şifrelemeye Giriş
11	Blok şifrelemeden EBM-çoklu güvenliğe kadar çoklu şifreleme güvenliği, determinizmin tuzakları, EBM güvenliği
12	Ayrık günlük problemine giriş ve Diffie-Hellman anahtar paylaşımı
13	Açık Anahtarlı Şifreleme, ElGamal, iyi ayrık günlük ayarları
14	RSA testi ve mini frekans aracı
15	Pollard'ın p-1 ve Pollard'ın Rho faktoring teknikleri, Trivium ve RC4 / Spritz

Dersin Program Çıktılarına Katkısı (1-5)

	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**
1	5	5	4			3	1
2	5	5	4			3	1
3	5	5	4			3	1
4	5	5	4			3	1
5	5	5	3			3	1

Katkı Oranı: 1: Çok Düşük 2: Düşük 3: Orta 4: Yüksek 5: Çok Yüksek

Hazırlayan:	MSc. Melce Hüsünbeyi

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
DERS BİLGİ FORMU

Güncelleme Tarihi:	12.03.2020