MATEMATİK BÖLÜMÜ YENİ SEÇMELİ DERS TEKLİF FORMU

Dersin Adı	Kriptoloji	
Kodu:----------	**Kredisi:**4	**AKTS:**6
Yıl / Yarıyıl	4. sınıf / Güz Yarıyılı	
Ders Düzeyi	**Lisans**	
Yazılım Şekli(Zorunlu/Seçmeli)	Seçmeli	
Ön Koşul	Yok	
Eğitim Sistemi	**Yüz yüze**	
Dersin Süresi	**14 Hafta /Haftada 4 saat teorik**	
Öğretim Üyesi	Dr. Öğr. Üyesi Şerife YILMAZ	
Diğer Öğretim Üyesi		
Öğretim Dili	**Türkçe**	

Dersin Amacı:

Dersin amacı öğrencilere kriptografi hakkında temel bilgileri ve kavramları öğretmek, öğrencilerin kriptografinin temel prensipleri ve veri şifreleme konusundaki uygulamaları hakkında bilgi sahibi olmalarını sağlamaktır.

Öğrenim Kazanımları		**PÖKK**	**ÖY**
Bu dersi başarı ile tamamlayan öğrenciler:			
ÖK - 1 :	Kriptoloji tarihi hakkında bilgi sahibi olacaklar	1,3	1
ÖK - 2 :	Kriptografik algoritmaların sınıflandırması konusunda bilgi sahibi olacaklar	1,3	1
ÖK - 3 :	Klasik ve modern kriptografi yöntem ve tekniklerini teorik ve pratik uygulamalarla öğrenecekler	1,3	1
ÖK - 4 :	Simetrik ve asimetrik kriptografik algoritmaları ve uygulamalarını öğrenecekler	1,3,5	1
ÖK 5 :	Örnek uygulamalar ile öğrendiklerini pekiştirecekler	1,3,5	1
PÖKK :Program öğrenim kazanımlarına katkı, ÖY : Ölçme ve değerlendirme yöntemi (1: Yazılı Sınav, 2: Sözlü Sınav, 3: Ev Ödevi, 4: Laboratuvar Çalışması/Sınavı, 5: Seminer / Sunum, 6: Dönem Ödevi / Proje),ÖK : Öğrenim Kazanımı			

Ders İçeriği

Modüler aritmetik, kriptolojinin tarihçesi, simetrik şifreleme yöntemleri, asimetrik şifreleme yöntemleri, Sezar yöntemi, Affine yöntemi, Vigenere Yöntemi, Vernam yöntemi, Hill yöntemi, Playfair Yöntemi, DES, AES, RSA, El Gamal yöntemleri, Eliptik eğri şifreleme algoritması.

Hafta	Detaylı İçerik
Hafta 1	Sayılar Teorisinde Hatırlatmalar
Hafta 2	Kriptolojiye Giriş
Hafta 3	Kriptografi Sistemlerinin Sınıflandırmaları
Hafta 4	Klasik Kriptografi Sistemleri
Hafta 5	Klasik Kriptografi Sistemleri-2
Hafta 6	Modern Kriptografi Sistemleri
Hafta 7	Simetrik Şifreleme(Gizli Anahtar) Algoritmaları
Hafta 8	AES Kripto Sistemi ve Uygulamaları
Hafta 9	ARA SINAV
Hafta 10	DES Kripto Sistemi ve Uygulamaları
Hafta 11	Asimetrik Şifreleme(Açık Anahtar) Algoritmaları
Hafta 12	RSA Kripto Sistemi ve Uygulamaları
Hafta 13	El Gamal Kripto Sistemi ve Uygulamaları
Hafta 14	Eliptik Eğri Kriptografisi
Hafta 15	Genel Tekrar
Hafta 16	DÖNEM SONU SINAVI

Ders Kitabı / Malzemesi

1	An Introduction to Cryptography, H.R. Kenneth, Second Edition, Discrete Mathematics and Its Applications, 2007.
2	

İlave Kaynak

1	Cryptography and Network Security, Third Edition, New Jersey, 2003.
2	

Ölçme ve Değerlendirme Y	Hafta	Tarih	Süre (Saat)	Katkı(%)	H
Arasınav	9. hafta			50	
Kısa Sınav					
Dönem Sonu Sınavı	16. hafta			50	

İşlem Yükü/ İşlem Adı	Haftalık Süre (saat)	Hafta Sayısı	Dönem Toplamı
Yüz yüze eğitim	4	14	56
Sınıf dışı çalışma	5	14	70
Ara sınav için hazırlık	15	1	15
Ara sınav	2	1	2
Dönem sonu sınavı için hazırlık	20	1	20
Dönem sonu sınavı	2	1	2
Toplam Çalışma Yükü			165