AYDIN ADNAN MENDERES ÜNİVERSİTESİ
DERS BİLGİ FORMU

Dersin Adı	Kriptoloji								
Ders Kodu	MTK560		Ders Düzeyi	Yüksek Lisans					
AKTS Kredi	8	İş Yükü	200 *(Saat)*	Teori	3	Uygulama	0	Laboratuvar	0
Dersin Amacı	Öğrenciye kriptoloji hakkında temel bilgileri kazandırmak ve günümüze kadar olan gelişmelerin neler olduğunu öğretmektir. Kriptoloji ile ilgili algoritmalar öğretilip bu algoritmalar kullanılarak uygulamalar geliştirilecektir.								
Özet İçeriği	Kriptografiye giriş. Kriptografi tarihçesi. Klasik kriptografi tarihçesi. Simetrik algoritmalar. Data Encryption Standard (DES). Asimetrik algoritmalar. Rivest, Shamir, Adleman algoritması (RSA). El Gamal Algoritması. Dijital imza standardı. Kriptografik protokoller.								
Staj Durum	Yok								
Öğretim Yöntemleri	Anlatım (Takrir), Tartışma, Bireysel Çalışma								
Dersi Veren Öğretim Elemanı(ları)									

Ölçme ve Değerlendirme Araçları		
Araç	Adet	Oran (%)
Ara Sınav (Vize)	1	30
Dönem Sonu Sınavı (Final)	1	50
Ödev	1	20

Ders Kitabı / Önerilen Kaynaklar	
1	Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1995, ISBN 978-0471117094.
2	Şifreleme Matematiği: Kriptografi, Ortadoğu Teknik Üniversitesi, Toplum Bilim Merkezi, Canan Çimen, Sedat Akleylek, Ersan Akyıldız, 2007, ISBN 978-9944-344-27-2.

Hafta	Haftalara Göre Ders Konuları	
1	Teorik	Kriptografiye giriş
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
2	Teorik	Kriptografi tarihçesi
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
3	Teorik	Klasik Kriptoloji metodları
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
4	Teorik	Klasik Kriptoloji metodları
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
5	Teorik	Simetrik algoritmalar
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
6	Teorik	Simetrik algoritmalar
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
7	Teorik	Data Encryption Standard (DES)
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
8	Teorik	Asimetrik algoritmalar
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
9	Teorik	Asimetrik algoritmalar
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
10	Ön Hazırlık	İşlenen tüm konular tekrarlanmalı
	Ara Sınav (Vize)	ARASINAV
11	Teorik	Rivest, Shamir, Adleman algoritması (RSA)
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
12	Teorik	El Gamal Algoritması
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
13	Teorik	Dijital imza standardı

13	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
14	Teorik	Kriptografik protokoller
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
15	Teorik	Kriptografik protokoller
	Ön Hazırlık	Ders kitabındaki ilgili konular okunmalı
16	Ön Hazırlık	İşlenen tüm konular tekrarlanmalı
	Dönem Sonu Sınavı (Final)	FİNAL

Dersin Öğrenme, Öğretme ve Değerlendirme Etkinlikleri Çerçevesinde İş Yükü Hesabı (Ortalama Saat)				
Etkinlik	Adet	Ön Hazırlık	Etkinlik Süresi	Toplam İş Yükü
Kuramsal Ders	14	3	3	84
Ödev	1	20	2	22
Ara Sınav	1	40	2	42
Dönem Sonu Sınavı	1	50	2	52
			Toplam İş Yükü (Saat)	200
			Yuvarla [Toplam İş Yükü (saat) / 25*] = **AKTS Kredisi**	8
**25 saatlik iş yükü 1 AKTS olarak kabul edilmektedir.*				

Dersin Öğrenme Çıktıları	
1	Kriptoloji kavramlarını anlamak
2	Kriptoloji algoritmalarını öğrenmek
3	Kriptoloji algoritmalarıyla uygulamalar geliştirebilmek
4	Öğrendiği matematiksel kavramlar arasındaki ilişkileri yorumlayabilme
5	Kurduğu matematiksel ilişkileri karşılaşabileceği problemleri çözmek için uygulayabilme

Program Çıktıları *(Matematik Tezsiz Yüksek Lisans Programı)*	
1	Lisans düzeyi yeterliliklerine dayalı olarak, alan bilgilerini uzmanlık düzeyinde geliştirebilmek.
2	Matematiğin ilişkili olduğu disiplinler arası etkileşimi kavrayabilmek.
3	Alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilmek.
4	Matematik alanındaki bilgilerini farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilmek ve yeni bilgiler üretebilmek.
5	Matematik alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilmek.
6	Matematik ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilmek.
7	Matematik ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilmek ve sorumluluk alarak çözüm üretebilmek.
8	Alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilmek.
9	Alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilmek
10	Matematik'deki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel verilerle destekleyerek alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde aktarabilmek.
11	Bir yabancı dili kullanarak sözlü ve yazılı iletişim kurabilmek.
12	Matematiğin gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilmek.
13	Matematik ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamasında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilmek ve değerleri öğretebilmek.
14	Matematik ile ilgili konularda strateji, politika ve uygulama planları geliştirebilmek ve elde edilen sonuçları kalite süreçleri çerçevesinde değerlendirebilmek.
15	Matematik alanında özümsedikleri bilgiyi, problem çözme ve uygulama becerilerini disiplinlerarası çalışmalarda kullanabilmek.

Program ve Öğrenme Çıktıları İlişkisi *1:Çok Düşük, 2:Düşük, 3:Orta, 4:Yüksek, 5:Çok Yüksek*

	ÖÇ1	ÖÇ2	ÖÇ3	ÖÇ4	ÖÇ5
PÇ1	2	3	3	3	3
PÇ2	3	4	4	4	4
PÇ3	4	5	5	5	5
PÇ4	3	4	4	4	4
PÇ12	3	4	4	4	4
PÇ15	4	4	4	4	4