ESOGÜ Matematik ve Bilgisayar Bilimleri Bölümü Ders Bilgi Formu

DÖNEM	Bahar

DERSİN KODU	821618001	DERSİN ADI	Kriptoloji

YARIYIL	HAFTALIK DERS SAATİ			DERSİN			
	Teorik	Uygulama	Laboratuar	Kredisi	AKTS	TÜRÜ	DİLİ
8	3	0	0	3	5	ZORUNLU (x) SEÇMELİ ( )	Türkçe

DERSİN KATEGORİSİ		
Matematik	Bilgisayar	Sosyal Bilim
x	x	

DEĞERLENDİRME ÖLÇÜTLERİ			
	Faaliyet türü	Sayı	%
YARIYIL İÇİ	Ara Sınav	1	40
	Ek Sınav		
	Kısa Sınav		
	Ödev		
	Proje		
	Rapor		
	Diğer (……)		
YARIYIL SONU SINAVI		1	60

VARSA ÖNERİLEN ÖNKOŞUL(LAR)	Yok.
DERSİN KISA İÇERİĞİ	Temel şifreleme sistemleri: genel prensipler, tek alfabeli ve çok alfabeli sistemler, basit analiz yöntemleri. Açık anahtarlı sistemlerin genel özellikleri. Blok ve akan şifre sistemlerinin genel özellikleri. Boole fonksiyonlarının genel yapısı. Sıkıştırma fonksiyonları ve doğrulama kodları.
DERSİN AMAÇLARI	Kriptoloji hakkında temel bilgiler vermek, kriptolojinin güncel uygulamalardaki yerini görmek ve bilinen temel kriptografi algoritmalarını görmek.
DERSİN MESLEK EĞİTİMİNİ SAĞLAMAYA YÖNELİK KATKISI	Kriptolojinin güncel uygulamalardaki yerini öğrenebilmek ve uygulayabilmek.
DERSİN ÖĞRENİM ÇIKTILARI	Kriptoloji hakkında genel bir bilgi sahibi olmak ve temel kriptografi algoritmalarını öğrenebilmek.
TEMEL DERS KİTABI	Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
YARDIMCI KAYNAKLAR	Neal Koblitz, "A Course in Number Theory and Crytography", Graduate Text in Mathematics, Springer Verlag, 1987. Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, 2002. Johannes Buchmann, "Introduction to Cryptography", Springer-Verlag, New York, 2001. Richard A. Mollin, "RSA and Public-Key Cryptography", Chapman & Hall/CRC, Boca Raton, 2003.
DERSTE GEREKLİ ARAÇ VE GEREÇLER	Yok.

DERSİN HAFTALIK PLANI	
HAFTA	**İŞLENEN KONULAR**
1	Temel şifreleme sistemleri
2	Temel şifreleme sistemleri ve analizleri
3	Sayılar teorisi ve sonlu cisimler
4	Açık anahtarlı sistemler
5	Açık anahtarlı sistemler
6	Boole fonksiyonları
7	Boole fonksiyonları
8	Arasınav
9	Blok şifre sistemleri
10	Blok şifre sistemleri
11	Blok şifre sistemleri
12	Akan şifre sistemleri
13	Akan şifre sistemleri.
14	Sıkıştırma fonksiyonları ve doğrulama kodları.
15	Sıkıştırma fonksiyonları ve doğrulama kodları.
16,17	Final Sınavı

NO	PROGRAM ÇIKTISI	3	2	1
1	Matematik ve bilgisayar bilimleri bilgilerini uygulama becerisi,	x		
2	Matematik alanında uluslararası düzeyde teori ve uygulamada yeterli bilgi birikimine sahip olmak,	x		
3	Matematik ve ilgili alanlarda matematiksel problemleri tanımlama, modelleme ve çözme becerisi,		x	
4	Tanımlanmış bir hedef doğrultusunda var olan problem sürecini çözümleme ve tasarlama becerisi,		x	
5	Verilerin çözümlenmesi, yorumlanması ve yorumlamayı diğer verilere uygulama ve bu bilgileri bilgisayar ortamında uygulayabilme becerisi	x		
6	Matematik uygulamaları için gerekli çağdaş teknikleri ve hesaplama araçlarını kullanabilme becerisi,	x		
7	Disiplin içi ve disiplinler arası takım çalışmasını yapabilme becerisi	x		
8	Matematik ve bilgisayar bilimlerinin yanı sıra diğer bilimsel, teknolojik ve çağdaş konular hakkındaki gelişmeleri izleyerek kendini geliştirme becerisi,		x	
9	Bireysel çalışma, analitik düşünme ve bağımsız karar verebilme yeteneğine sahip olarak fikirlerini sözlü ve yazılı, açık ve öz bir şekilde ifade ederek iletişim kurabilme becerisi,		x	
10	Mesleki ve etik sorumluluk bilincine sahip olma becerisi,		x	
11	Bilimsel araştırma ve kalite konularında bilinç sahibi olma becerisi,		x	
12	Yaşadığı çevrenin sorunlarına ve gelişimine yönelik duyarlı ve sosyal ilişkilerde tutarlı olabilme becerisi,		x	
13	Karşılaştığı problemleri çözebilmek için problem çözme ve matematiksel modelleme yoluyla uygun algoritmalar kullanabilme ve bilgisayar programı yazabilme becerisi,	x		
14	Farklı karmaşıklık düzeyindeki yazılım sistemlerinin oluşturulmasında tasarım ve geliştirme becerisi,	x		
15	Yaşam boyu öğrenmenin gerekliliğini takdir etme ve yaşam boyu öğrenimi uygulama becerisi.		x	
1:Hiç Katkısı Yok. **2**:Kısmen Katkısı Var. **3**:Tam Katkısı Var.				

Dersin Öğretim Üyesi: Prof. Dr. İ. İlker Akça

İmza: **Tarih:**