BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN FAKÜLTESİ

MATEMATİK

(2024 - 2025) Ders Bilgi Formu

Ders Adı	Kodu	Yarıyıl	T+U Saat	AKTS	Z / S
Matematik Şifreleme	MAT428	8	2 + 1	6,0	Seçmeli

Birim Bölüm	Matematik - Lisans (Yüz yüze)
Amaç	Lisans seviyesindeki öğrencilere kriptografinin temel prensiplerini, şifreleme ve sayısal imza gibi güvenlik uygulamalarının temellerini öğretmek ve bu konularda yeni yetenekler kazandırmak olarak belirlenmiştir.
Ders İçeriği	Matematiksel temeller, blok şifreleme algoritmaları, rastgele sayı üreticileri ve akan veri şifreleyicileri, tek yönlü hash algoritmaları, açık anahtarlı kripto sistem algoritmaları, tanımlama ve anahtar değişimi algoritmaları, güvenli haberleşme teknikleri, açık ve kapalı anahtar kripto sistemleri, sayısal imzalama, kimlik tanıma ve tanıtma yöntemleri ve güvenlik protokolleri.
Ders Kaynakları	Cryptography Network Security: Principal and Practice, W.Stallings, 2013

Hafta	Konu
1	Temel Kavramlar
2	Kriptografide Matematik
3	Geleneksel Şifreleme Yöntemleri
4	Geleneksel Şifreleme Yöntemleri
5	Modern Kriptografi
6	Modern Kriptografi
7	Kimlik Doğrulama
8	Anahtar Yönetimi
9	Özetleme Fonksiyonları
10	Sayısal İmzalar
11	Ağ ve Yazılım Güvenliği Politikaları
12	Giz paylaşımı ve diğer konular
13	Proje sunumları
14	Proje sunumları

Program Çıktıları	
1	Matematik alanındaki güncel bilgileri içeren bilimsel kaynaklarla desteklenen ileri düzeydeki kuramsal ve uygulamalı bilgilere sahip olur.
2	Matematik bilimindeki kavramları, teorileri ve verileri, bilimsel yöntemlerle değerlendirerek, karşılaşılan problem ve konuları belirleme ve analiz etme, tartışmalar yapma, kanıta ve araştırmalara dayalı öneriler geliştirme becerisine sahiptir.
3	Matematik problemlerini çözebilmek için gerekli analitik düşünme, soyut düşünme, yayın araştırması ve diğer kaynakları kullanma becerisine sahiptir.
4	Alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini kullanabilme yetkinliğine sahip olur.
5	Matematik problemlerini çözmek için gerekli olan uygun yöntemleri ve teknikleri seçme, ispat tekniklerini kullanabilme ve çözüm için karar verme becerisine sahiptir.
6	Bireysel ve gruplarla (takım halinde) etkin çalışabilme becerisi, sorumluluk alma özgüvenine sahiptir.
7	Yaşam boyu öğrenmenin gerekliliği bilincine sahip olur; matematik ve diğer bilim dallarındaki gelişmeleri izler ve kendi sürekli olarak yeniler.
8	Matematik bilimindeki bilgileri takip edebilecek ve paydaşları ile iletişim kurabilecek düzeyde bir yabancı dil bilgisine sahiptir.
9	Alanı ile ilgili konularda düşüncelerini ve konulara ilişkin çözüm önerilerini yazılı ve sözlü olarak aktarabilme becerisine sahiptir.
10	Matematik bilimi ile ilgili verilerin toplanması, yorumlanması, duyurulması aşamalarında toplumsal, bilimsel ve etik değerlere sahiptir.
11	Girişimcilik ve yenilikçilik tarafını sürekli geliştirme, matematiksel çözümlerin ve uygulamaların evrensel ve toplumsal boyutlardaki etkilerinin bilincinde olmak, çağın sorunları hakkında bilgi sahibidir.

Ders Öğrenme Çıktısı - Program Çıktıları (1 -5 Puan Aralığı)

Ders Öğrenme Çıktısı	PÇ 1	PÇ 2	PÇ 3	PÇ 4	PÇ 5	PÇ 6	PÇ 7	PÇ 8	PÇ 9	PÇ 10	PÇ 11
Temel kriptografi kavramlarını tanımlar	-	-	-	-	-	-	-	-	-	-	-
Kriptografinin temel matematiksel kavramlarını açıklar	-	-	-	-	-	-	-	-	-	-	-
Şifreleme algoritmaları konusunda teorik ve pratik bilgi ve deneyim kazandırır	-	-	-	-	-	-	-	-	-	-	-
Açık anahtarlamalı kriptografik sistemlerin temel prensiplerini listeler	-	-	-	-	-	-	-	-	-	-	-
Sayısal imza algoritmaları konusunda teorik ve pratik bilgi ve deneyim kazandırır	-	-	-	-	-	-	-	-	-	-	-
Ortalama Değer	-	-	-	-	-	-	-	-	-	-	-