

İndirilme Tarihi

05.02.2026 14:36:03

MAT494 - KRİPTOLOJİYE GİRİŞ - Fen Edebiyat Fakültesi - Matematik Bölümü

Genel Bilgiler

Dersin Amacı

Bu dersin amacı, öğrencilere klasik ve modern kriptosistemler hakkında temel bilgiler kazandırmak. Bu sistemlerin uygulama alanlarının önemini ortaya koymak ve açık anahtar kriptosistemleri ile bu sistemlere yönelik ataklar konusunda bir altyapı oluşturmaktır.

Dersin İçeriği

Kriptolojinin Amacı ve Kriptosistemin Tanımı, Sezar Kriptosistemi, Afin Kriptosistemi, Yerdeğiştirme Kriptosistemi, Vigenere Kriptosistemi, Hill Kriptosistemi, Kripto Analiz, Sayılar Teorisi ile İlgili Ön bilgiler, Diffie-Hellman Anahtar Belirleme Yöntemi, Ardışık Kare Alma Yöntemi, El-Gamal Kriptosistemi, Normal Bölme ile Çarpanlara Ayırma Yöntemi, Fermat Çarpanlara Ayırma Yöntemi, RSA Kriptosistemi, Telefonda Yazı Tura Oyunu

Dersin Kitabı / Malzemesi / Önerilen Kaynaklar

Altındış, H., Sayılar Teorisi ve Uygulamaları, Palme Yayıncılık, Ankara, 2011.

Planlanan Öğrenme Etkinlikleri ve Öğretme Yöntemleri

Ders İçin Önerilen Diğer Hususlar

Dersi Veren Öğretim Elemanı Yardımcıları

Dersin Verilişi

Dersi Veren Öğretim Elemanları

Dr. Öğr. Üyesi Hayrullah Özımamoğlu

Program Çıktısı

- Kriptolojinin amacını ve temel kriptosistemleri açıklamak.
- Sezar, Afin, Yerdeğiştirme, Vigenere ve Hill kriptosistemlerinin çalışma mantığını kavramak
- Kripto analiz sürecini ve sayılar teorisiyle ilişkili ön bilgileri anlamak.
- Diffie-Hellman, El-Gamal ve RSA kriptosistemlerinin anahtar oluşturma ve güvenlik yapılarını karşılaştırmak.
- Ardışık kare alma, normal bölme, Fermat çarpanlara ayırma yöntemlerini ve telefonda yazı tura oyununu öğrenmek.

Haftalık İçerikler

Sıra	Hazırlık Bilgileri	Laboratuvar	Öğretim Metodları	Teorik	Uygulama
1				Kriptolojinin Amacı ve Kriptosistemin Tanımı	
2				Sezar Kriptosistemi	
3				Afin Kriptosistemi	
4				Yerdeğiştirme Kriptosistemi	
5				Vigenere Kriptosistemi	
6				Hill Kriptosistemi	
7				Kripto Analiz	
8				Ara Sınav	
9				Sayılar Teorisi ile İlgili Ön bilgiler	
10				Diffie-Hellman Anahtar Belirleme Yöntemi	
11				Ardışık Kare Alma Yöntemi	
12				El-Gamal Kriptosistemi	
13				Normal Bölmeyle ve Fermat Çarpanlara Ayırma Yöntemi	
14				RSA Kriptosistemi	
15				Telefonda Yazı Tura Oyunu	

Aktiviteler	Sayısı	Süresi (saat)
Teorik Ders Anlatım	14	3,00
Ders Öncesi Bireysel Çalışma	14	2,00
Ders Sonrası Bireysel Çalışma	14	5,00
Ara Sınav Hazırlık	4	4,00
Vize	1	2,00
Final Sınavı Hazırlık	4	5,00
Vaka Çalışması	0	0,00
İnceleme/Anket Çalışması	0	0,00
Final	1	2,00

Değerlendirme

Aktiviteler	Ağırlığı (%)
Ara Sınav	40,00
Final	60,00

Matematik Bölümü / MATEMATİK X Öğrenme Çıktısı İlişkisi

	P.Ç. 1	P.Ç. 2	P.Ç. 3	P.Ç. 4	P.Ç. 5	P.Ç. 6	P.Ç. 7	P.Ç. 8	P.Ç. 9	P.Ç. 10	P.Ç. 11
Ö.Ç. 1	5	5									
Ö.Ç. 2	5	5									
Ö.Ç. 3	5	5									
Ö.Ç. 4	5	5									
Ö.Ç. 5	5	5									

Tablo :

- P.Ç. 1 :** Matematiğin temel alanlarından Analiz, Geometri ve Cebirin temel kavramlarını bilimsel yöntem ve teknikler yardımıyla tanımlar.
- P.Ç. 2 :** Matematiksel verileri yorumlar, çözümler, güvenilirliğini ve geçerliliğini değerlendirir.
- P.Ç. 3 :** Günlük hayattaki bazı problemlerin Matematiksel modellerini tanımlar, eleştirel bir açı ile değerlendirir, teorik ve uygulamalı bilgilerle analiz eder.
- P.Ç. 4 :** Öğrenme süreçlerinde disiplinler arası yaklaşımı analitik olarak kullanır.
- P.Ç. 5 :** Matematik alanındaki bir konuya uygun materyal geliştirir; bilgi ve tecrübe kazanımlarını farklı yöntemlerle kullanır.
- P.Ç. 6 :** Kendini bir birey olarak tanıır; yaratıcı ve güçlü yönlerini kullanır, kişisel ve kurumsal iletişim ve etkileşim kurar.
- P.Ç. 7 :** Alanıyla ilgili öğrenme ihtiyaçlarını belirler. Alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde etkileşimli olarak kullanır.
- P.Ç. 8 :** Yaşam boyu öğrenme ve kalite yönetim süreçlerini öğrenir ve uygular; alanındaki sosyal, kültürel ve sanatsal etkinliklere katılır.
- P.Ç. 9 :** Toplumsal sorumluluk bilinciyle mesleki proje ve etkinlikler planlar ve uygular.
- P.Ç. 10 :** Matematik temel alanının gerektirdiği yabancı dili Avrupa Dil Portföyü B1 Genel düzeyinde kullanarak sözlü ve yazılı iletişim kurar.
- P.Ç. 11 :** Kazanacağı bilgi birikimi ile sorumluluğu altında çalışanların öğrenme gereksinimlerini belirler, lisansüstü eğitimin gereklerini yerine getirir.
- Ö.Ç. 1 :** Kriptolojinin amacını ve temel kriptosistemleri açıklamak.
- Ö.Ç. 2 :** Sesar, Afin, Yerdeğiştirme, Vigenere ve Hill kriptosistemlerinin çalışma mantığını kavramak
- Ö.Ç. 3 :** Kripto analiz sürecini ve sayılar teorisiyle ilişkili ön bilgileri anlamak.
- Ö.Ç. 4 :** Diffie-Hellman, El-Gamal ve RSA kriptosistemlerinin anahtar oluşturma ve güvenlik yapılarını karşılaştırmak.
- Ö.Ç. 5 :** Ardışık kare alma, normal bölme, Fermat çarpanlara ayırma yöntemlerini ve telefonda yazı tura oyununu öğrenmek.