2023 - 2024 Akademik Yılı Güz Doç.Dr. Sait TAŞ FMT223 Şifrelemeye Giriş

Dersin tanımı

Ön koşul dersleri	:	
Eğitimin dili	:	Türkçe
Dersi veren öğretim eleman(lar)ı	:	Doç.Dr. Sait TAŞ
Yardımcı öğretim eleman(lar)ı	:	
Dersin veriliş şekli	:	Yüzyüze
Dersin amacı	:	Bazı Şifreleme yöntemleri hakkında bilgi sahibi olmak.
Dersin tanımı	:	Bazı Şifreleme yöntemleri hakkında bilgi sahibi olmak ve uygulamalarını yapabilmektir.

Dersin içeriği

Sıra	İçerik
1	Giriş- Kriptografi Tarihi
2	Sayılar Teorisine Giriş
3	Sayılar Teorisine Giriş Devam
4	Grup-Halka-Cisim Teorisi
5	Grup-Halka-Cisim Teorisi devam
6	Karakter şifreleme
7	Karakter şifreleme devam
8	Blok şifreleme
9	Blok şifreleme devam
10	Üslü şifreleme
11	Üslü şifreleme devam
12	Açık Anahtar şifreleme
13	Knapsack Açık anahtar şifreleme
14	Genel tekrar
15	Final

Dersin öğrenme çıktıları

Sıra	İçerik
1	Şifreleme temel kavramlarını ve mantığını tanır.
2	Simetrik ve Asimetrik Şifreler hakkında bilgi verir.

Sıra	İçerik
3	Şifreleme uygulamalarını yapabilir.
4	Kriptanaliz hakkında bilgi verir.

Dersin program yeterliliklerine katkı seviyesi

Yeterlilik	Puan
Matematiksel kavramlar ve prensiplerin geniş bir çeşitliliğini harmanlamak, benimsemek ve anlamak.	4
Diğer disiplinler üzerinde matematiğin etkili olduğu konuların farkına varmak ve anlamak.	4
Diğer disiplinlerle ilgili temel bilgileri kazanmak.	4
Matematiksel ve sayısal hesaplama yeteneklerinin gelişimini sağlamak.	4
Teorik bilgiyi yorumlamak ve uygun sonuçları çıkarmak.	4
Matematiksel odaklı bilgisayar programlarını kullanmak.	4
Temel kaynakları okumak ve yorumlamak.	4
Kişisel sorumluluk kazanmak.	4
Matematiğin lisansüstü konularında ulusal ve uluslar arası düzeyde çalışmaları bağımsız olarak yürütüp, ortaklaşa çalışmalar yapabilmek	4
Kendi başına çalışma ve çeşitli ortamlarda problem çözme ve teorem ispatlama bilgi birikimine sahip olmayı kazanmak.	4
Doğru ve güvenli teorik ve uygulamalı araştırma yapmak.	4
Diğer disiplinlerdeki kişilerle etkileşip, bir takımda çalışma yeteneğini geliştirmek.	4
Yazılı ve sözlü raporlar ve sunumlar yoluyla etkileşim ve iletişim kurabilme yeteneğini kazanmak.	4
Mesleki ve bilimsel etik değerlere saygılı bir kişiliğe sahip olmak	4
Matematiksel düşünmeyi hayatının her alanında kullanabilmek	4
Gerçek dünya problemlerinde Matematiksel prensipleri uygulayabilme	4

Dersin kurumsal yeterliliklerine katkı seviyesi

Yeterlilik	Puan
DİJİTALLEŞME	
Alanıyla ilişkili dijital teknolojileri ve ortamları dijital güvenlik ve etik kurallar çerçevesinde kullanma ve geliştirme becerisi kazanır.	3
DİSİPLİNLERARASI OLMA	
Alanının diğer alanlarla ilişkisini kurar ve disiplinlerarası çalışabilme becerisi kazanır.	3
TOPLUMA KATKI	

Yeterlilik	Puan
Toplumsal sorunlara yönelik çözümler üretir ve paylaşır.	3
GİRİŞİMCİLİK	
Toplumsal ihtiyaçlara yönelik girişimci fikirler (araştırma, sosyal, üretim vb.) geliştirir ve uygular.	3
ULUSLARARASILAŞMA	
Uluslararası ölçekte alanıyla ilişkili çalışmaları takip ederek katkı sağlama ve işbirliği yapma amacıyla bir yabancı dili kullanma yeterliği kazanır.	3

Planlanan öğretim faaliyetleri, öğretme metodları ve AKTS iş yükü

	Sayısı	Süresi (saat)	Sayı*Süre (saat)
Yüz yüze eğitim	14	3	42
Sınıf dışı ders çalışma süresi (ön çalışma, pekiştirme)	14	1	14
Ödevler	7	1	7
Sunum / Seminer hazırlama	0	0	0
Kısa sınavlar	0	0	0
Ara sınavlara hazırlık	4	1	4
Ara sınavlar	1	1	1
Proje (Yarıyıl ödevi)	0	0	0
Laboratuvar	0	0	0
Arazi çalışması	0	0	0
Yarıyıl sonu sınavına hazırlık	5	1	5
Yarıyıl sonu sınavı	1	2	2
Araştırma	0	0	0
Toplam iş yükü			75
AKTS			3

Değerlendirme yöntemleri ve kriterler

Değerlendirme	Katkı Yüzdesi
Ara Sınav	40.0
Yarıyıl Sonu	60.0
Bütünleme	60.0

Önerilen veya zorunlu okuma materyalleri

Ders kitabı	:	Sayılar Teorisi ve Uygulamaları; Hüseyin Altındiş, Cryptography Theory and Practice (Douglas R. Stinson), Understanding Cryptography (Christof Paar)
Yardımcı Kaynaklar	: