MAT519 - KRİPTOLOJİ I - Fen Bilimleri Enstitüsü - Matematik Ana Bilim Dalı

Genel Bilgiler

Dersin Amacı

Bu dersin amacı, klasik ve modern kriptografi tekniklerini, bunların kriptoanaliz yöntemlerini ve ilgili sayısal algoritmaları inceleyerek şifreleme ve şifre çözme süreçlerinin matematiksel temellerini kavramaktır.

Dersin İçeriği

Kaydırma Şifrelemesi, Yerine Koyma Şifrelemesi, Afin Şifrelemesi, Vigenere Şifrelemesi, Permütasyon Şifrelemesi, Akış Şifrelemesi, Hill Şifrelemesi, Afin Şifrelemesinin Kriptoanalizi, Yerine Koyma Şifrelemesinin Kriptoanalizi, Vigenere Şifrelemesinin Kriptoanalizi, Hill Şifrelemesinin Kriptoanalizi, LFSR Akış Şifrelemesinin Kriptoanalizi, Öklid Algoritması, Çin Kalan Teoremi, Diğer Yararlı Bilgiler, RSA Kriptosistemi, Legendre Sembolleri, Jacobi Sembolleri, Solovay-Strassen Algoritması, Miller-Rabin Algoritması, n Modülünde Kare Kökler, Pollard p-1 Algoritması, Pollard Rho Algoritması, Dixon'ın Rastgele Kare Algoritması, Uygulamada Çarpanlarına Ayırma Algoritmaları, Euler Phi Fonksiyonunun Hesaplanması, Şifre Çözme Üs Değeri, Wiener'ın Düşük Şifre Çözme Üs Değeri Saldırısı ve Rabin Kriptosistemi, Düz Metin Bitleri Hakkında Kısmi Bilgi, Optimal Asimetrik Şifreleme Dolgusu

Dersin Kitabı / Malzemesi / Önerilen Kaynaklar

Stinson, Douglas R., Cryptography: Theory and Practice, Chapman and Hall/CRC, 2005.

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 Özimamoğlu

Program Çıktısı

1. Klasik ve modern şifreleme tekniklerini (Kaydırma, Yerine Koyma, Afin, Vigenere, Permütasyon, Hill ve Akış şifrelemeleri) tanımlamak ve karşılaştırmak.
2. Kriptanaliz yöntemlerini (Affine, Substitution, Vigenère, Hill, LFSR akış şifreleri) uygulayarak şifreli metinlerin güvenliğini değerlendirmek.
3. Temel sayısal ve cebirsel algoritmaları (Öklid Algoritması, Çin Kalan Teoremi, Euler Phi Fonksiyonu, Pollard ve Dixon algoritmaları) kullanarak şifreleme ve şifre çözme süreçlerini analiz etmek.
4. Pratik uygulamalarda sayı teorisi ve olasılık temelli algoritmalar (Legendre, Jacobi sembolleri; Solovay-Strassen ve Miller-Rabin testleri) kullanarak güvenli anahtar üretimi ve şifreleme stratejilerini değerlendirmek.
5. RSA ve Rabin kriptosistemleri gibi modern asimetrik şifreleme yöntemlerinin matematiksel temellerini kavramak ve şifreleme/deşifreleme süreçlerini gerçekleştirmek.

Haftalık İçerikler

Sıra	Hazırlık Bilgileri	Laboratuvar	Öğretim Metodları	Teorik	Uygulama
1				Kaydırma Şifrelemesi ve Yerine Koyma Şifrelemesi	
2				Afin Şifrelemesi, Vigenere Şifrelemesi ve Hill Şifrelemesi	
3				Permütasyon Şifrelemesi ve Akış Şifrelemesi	
4				Afin Şifrelemesinin Kriptoanalizi ve Yerine Koyma Şifrelemesinin Kriptoanalizi	
5				Vigenere Şifrelemesinin Kriptoanalizi, Hill Şifrelemesinin Kriptoanalizi ve LFSR Akış Şifrelemesinin Kriptoanalizi	
6				Öklid Algoritması ve Çin Kalan Teoremi	
7				Diğer Yararlı Bilgiler ve RSA Kriptosistemi	
8				Ara Sınav	
9				Legendre Sembolleri, Jacobi Sembolleri ve Solovay-Strassen Algoritması	
10				Miller-Rabin Algoritması ve n Modülünde Kare Kökler	
11				Pollard p-1 Algoritması ve Pollard Rho Algoritması	
12				Dixon'ın Rastgele Kare Algoritması ve Uygulamada Çarpanlarına Ayırma Algoritmaları	
13				Euler Phi Fonksiyonunun Hesaplanması ve Şifre Çözme Üs Değeri	
14				Wiener'ın Düşük Şifre Çözme Üs Değeri Saldırısı ve Rabin Kriptosistemi	
15				Düz Metin Bitleri Hakkında Kısmi Bilgi ve Optimal Asimetrik Şifreleme Dolgusu	

İş Yükleri

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
Final	1	2,00

Değerlendirme

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

Matematik Ana Bilim Dalı / MATEMATİK (YÜKSEK LİSANS - TEZLİ) 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	P.Ç. 12	P.Ç. 13	P.Ç. 14	P.Ç. 15	P.Ç. 16	P.Ç. 17	P.Ç. 18
Ö.Ç. 1	5		5	5		5		5										5
Ö.Ç. 2	5		5	5		5		5										5
Ö.Ç. 3	5		5	5		5		5										5
Ö.Ç. 4	5		5	5		5		5										5
Ö.Ç. 5	5		5	5		5		5										5

Tablo :

P.Ç. 1 : Analiz, Uygulamalı matematiğin, Geometri ve Cebirin bazı alt toerileri hakkındaki temel teoremleri yeni problemlere uygulayabilir.

P.Ç. 2 : programcıktısı 2

P.Ç. 3 : Matematik, fen bilimleri ve kendi dalları ile ilgili konularda yeterli alt yapıya sahiptir ve bu alanlardaki teorik ve uygulamalı bilgileri jmatematik problemlerin çözümleri için kullanır.

P.Ç. 4 : Bilimsel, matematiksel düşünme yeteneği kazanabilme ve ilgili alanlarda bu bilgiyi kullanabilme.

P.Ç. 5 : Bilimsel, matematiksel düşünme yeteneği kazanabilme ve ilgili alanlarda bu bilgiyi kullanabilme.

P.Ç. 6 : Temel matematiksel beceriler (problem çözme, akıl yürütme, ilişkilendirme, genelleme) ve bu becerilere dayalı yetenekler edinebilme. (Rasyonel düşünme tekniği kazandırabilme)

P.Ç. 7 : Bilim ve teknolojideki gelişmeleri izleme ve kendini sürekli yenileme becerisi kazanabilme.

P.Ç. 8 : Bilgiye erişebilme ve bu amaçla kaynak araştırması yapabilme, veri tabanlarını ve diğer bilgi kaynaklarını kullanabilme becerisine sahip olabilme.

P.Ç. 9 : Çalışma hayatında etik sorumlulukların gereklerini yerine getirebilme.

P.Ç. 10 : Bilim tarihi ve bilimsel bilginin üretimiyle ilgili bilgi edinebilme.

P.Ç. 11 : Eleştirel ve yaratıcı düşünmenin ve problem çözme becerilerinin gelişimi için uygun yöntem ve tekniklerle etkinlikler düzenleyebilme.

P.Ç. 12 : Çalışma hayatı ve sosyal yaşam ile ilgili konularda bireysel ve takım çalışmaları yapabilme.

P.Ç. 13 : Alanı ile ilgili konularda düşüncelerini ve konulara ilişkin çözüm önerilerini yazılı ve sözlü olarak aktarabilme.

P.Ç. 14 : Matematiksel bilgi birikimlerini teknolojide kullanabilme.

P.Ç. 15 : Alanındaki bilgileri izleyebilecek ve meslektaşları ile iletişim kurabilecek düzeyde bir yabancı dili geliştirebilme.

P.Ç. 16 : Gerçek dünya problemlerinde Matematiksel prensipleri uygulayabilme.

P.Ç. 17 : Farklı disiplinlerin yaklaşım ve bilgilerini Matematikte kullanabilme.

P.Ç. 18 : Matematik alanındaki bir problemi, bağımsız olarak kurgulayabilme, çözüm yöntemi geliştirebilme, çözebilme, sonuçları değerlendirebilme ve gerektiğinde uygulayabilme.

Ö.Ç. 1 : Klasik ve modern şifreleme tekniklerini (Kaydırma, Yerine Koyma, Afin, Vigenere, Permütasyon, Hill ve Akış şifrelemeleri) tanımlamak ve karşılaştırmak.

Ö.Ç. 2 : Kriptanaliz yöntemlerini (Affine, Substitution, Vigenère, Hill, LFSR akış şifreleri) uygulayarak şifreli metinlerin güvenliğini değerlendirmek.

Ö.Ç. 3 : Temel sayısal ve cebirsel algoritmaları (Öklid Algoritması, Çin Kalan Teoremi, Euler Phi Fonksiyonu, Pollard ve Dixon algoritmaları) kullanarak şifreleme ve şifre çözme süreçlerini analiz etmek.

Ö.Ç. 4 : Pratik uygulamalarda sayı teorisi ve olasılık temelli algoritmalar (Legendre, Jacobi sembolleri; Solovay-Strassen ve Miller-Rabin testleri) kullanarak güvenli anahtar üretimi ve şifreleme stratejilerini değerlendirmek.

Ö.Ç. 5 : RSA ve Rabin kriptosistemleri gibi modern asimetrik şifreleme yöntemlerinin matematiksel temellerini kavramak ve şifreleme/deşifreleme süreçlerini gerçekleştirmek.