İndirilme Tarihi

05.02.2026 14:36:45

MAT494 - INTRODUCTION TO CRYPTOGRAPHY - Fen Edebiyat Fakültesi - Matematik Bölümü

General Info

Objectives of the Course

The aim of this course is to provide students with fundamental knowledge of classical and modern cryptosystems, to highlight the importance of their application areas, and to build a solid foundation on public-key cryptosystems and the attacks against these systems.

Course Contents

The Purpose of Cryptology and the Definition of a Cryptosystem, Caesar Cryptosystem, Affine Cryptosystem, Substitution Cryptosystem, Vigenere Cryptosystem, Hill Cryptosystem, Cryptanalysis, Preliminary Information Related to Number Theory, Diffie-Hellman Key Exchange Method, Successive Squaring Method, El-Gamal Cryptosystem, Factorization Method by Trial Division, Fermat Factorization Method, RSA Cryptosystem, Heads or Tails Game on the Phone

Recommended or Required Reading

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

Planned Learning Activities and Teaching Methods

_____

Recommended Optional Programme Components

_____

Instructor's Assistants

_____

Presentation Of Course

_____

Dersi Veren Öğretim Elemanları

Dr. Öğr. Üyesi Hayrullah Özimamoğlu

Program Outcomes

1. Explain the purpose of cryptology and basic cryptosystems.
2. Understand the working principles of the Caesar, Affine, Substitution, Vigenere, and Hill cryptosystems.
3. Understand the process of cryptanalysis and the preliminary knowledge related to number theory.
4. Compare the key generation and security structures of the Diffie-Hellman, El-Gamal, and RSA cryptosystems.
5. Learn the successive squaring method, trial division, the Fermat factorization method, and the heads-or-tails game on the phone.

Weekly Contents

Order	PreparationInfo	Laboratory	TeachingMethods	Theoretical	Practise
1				The Purpose of Cryptology and the Definition of a Cryptosystem	
2				Caesar Cryptosystem	
3				Affine Cryptosystem	
4				Substitution Cryptosystem	
5				Vigenere Cryptosystem	
6				Hill Cryptosystem	
7				Cryptanalysis	
8				Midterm Exam	
9				Preliminary Information Related to Number Theory	
10				Diffie-Hellman Key Exchange Method	
11				Successive Squaring Method	
12				El-Gamal Cryptosystem	
13				Factorization Method by Trial Division and Fermat	
14				RSA Cryptosystem	
15				Heads or Tails Game on the Phone	

Workload

Activities	Number	PLEASE SELECT TWO DISTINCT LANGUAGES
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

Assesments

Activities	Weight (%)
Ara Sınav	40,00
Final	60,00

Matematik Bölümü / MATEMATİK X Learning Outcome Relation

	P.O. 1	P.O. 2	P.O. 3	P.O. 4	P.O. 5	P.O. 6	P.O. 7	P.O. 8	P.O. 9	P.O. 10	P.O. 11
L.O. 1	5	5									
L.O. 2	5	5									
L.O. 3	5	5									
L.O. 4	5	5									
L.O. 5	5	5									

Table :

P.O. 1 : Matematiğin temel alanlarından Analiz, Geometri ve Cebirin temel kavramlarını bilimsel yöntem ve teknikler yardımıyla tanımlar.

P.O. 2 : Matematiksel verileri yorumlar, çözümler, güvenirliliğini ve geçerliliğini değerlendirir.

P.O. 3 : Günlük hayattaki bazı problemlerin Matematiksel modellerini tanımlar, eleştirel bir açı ile değerlendirir, teorik ve uygulamalı bilgilerle analiz eder.

P.O. 4 : Öğrenme süreçlerinde disiplinler arası yaklaşımı analitik olarak kullanır.

P.O. 5 : Matematik alanındaki bir konuya uygun materyal geliştirir; bilgi ve tecrübe kazanımlarını farklı yöntemlerle kullanır.

P.O. 6 : Kendini bir birey olarak tanır; yaratıcı ve güçlü yönlerini kullanır, kişisel ve kurumsal iletişim ve etkileşim kurar.

P.O. 7 : Alanıyla ilgili öğrenme ihtiyaçlarını belirler. Alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde etkileşimli olarak kullanır.

P.O. 8 : Yaşam boyu öğrenme ve kalite yönetim süreçlerini öğrenir ve uygular; alanındaki sosyal, kültürel ve sanatsal etkinliklere katılır.

P.O. 9 : Toplumsal sorumluluk bilinciyle mesleki proje ve etkinlikler planlar ve uygular.

P.O. 10 : Matematik temel alanının gerektirdiği yabancı dili Avrupa Dil Portföyü B1 Genel düzeyinde kullanarak sözlü ve yazılı iletişim kurar.

P.O. 11 : Kazanacağı bilgi birikimi ile sorumluluğu altında çalışanların öğrenme gereksinimlerini belirler, lisansüstü eğitimin gereklerini yerine getirir.

L.O. 1 : Kriptolojinin amacını ve temel kriptosistemleri açıklamak.

L.O. 2 : Sezar, Afin, Yerdeğiştirme, Vigenere ve Hill kriptosistemlerinin çalışma mantığını kavramak

L.O. 3 : Kripto analiz sürecini ve sayılar teorisiyle ilişkili önbilgileri anlamak.

L.O. 4 : Diffie-Hellman, El-Gamal ve RSA kriptosistemlerinin anahtar oluşturma ve güvenlik yapılarını karşılaştırmak.

L.O. 5 : Ardışık kare alma, normal bölme, Fermat çarpanlara ayırma yöntemlerini ve telefonda yazı tura oyununu öğrenmek.