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

General Info

Objectives of the Course

The aim of this course is to comprehend the mathematical foundations of encryption and decryption processes by examining classical and modern cryptographic techniques, their cryptanalysis methods, and the relevant numerical algorithms.

Course Contents

The Shift Cipher, the Substitution Cipher, theAffine Cipher, the Vigenere Cipher, the Permutation Cipher, the Stream Cipher, the Hill Cipher, Cryptanalysis of the Affine Cipher, Cryptanalysis of the Substitution Cipher, Cryptanalysis of the Vigenere Cipher, Cryptanalysis of the Hill Cipher, Cryptanalysis of the LFSR Stream Cipher, Euclidean Algorithm, Chinese Remainder Theorem, Other Useful Facts, RSA Cryptosystem, Legendre Symbols, Jacobi Symbols, Solovay-Strassen Algorithm, Miller-Rabin Algorithm, Square Roots Modulo n, Pollard p-1 Algorithm, Pollard Rho Algorithm, Dixon's Random Square Algorithm, Factoring Algorithms in Practice, Computing Euler Phi Function, Decryption Exponent, Wiener's Low Decryption Exponent Attack and the Rabin Cryptosystem, Partial Information Concerning Plaintext Bits, Optimal Asymmetric Encryption Padding

Recommended or Required Reading

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

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. Define and compare classical and modern cryptographic techniques (Shift, Substitution, Affine, Vigenere, Permutation, Hill, and Stream ciphers).
2. Apply cryptanalysis methods (Affine, Substitution, Vigenère, Hill, and LFSR stream ciphers) to evaluate the security of encrypted texts.
3. Analyze encryption and decryption processes using fundamental numerical and algebraic algorithms (Euclidean Algorithm, Chinese Remainder Theorem, Euler Phi Function, Pollard and Dixon algorithms).
4. Evaluate secure key generation and encryption strategies in practical applications using number-theoretic and probabilistic algorithms (Legendre and Jacobi symbols; Solovay-Strassen and Miller-Rabin tests).
5. Comprehend the mathematical foundations of modern asymmetric cryptosystems, such as RSA and Rabin, and perform encryption/decryption processes.

Weekly Contents

Order	PreparationInfo	Laboratory	TeachingMethods	Theoretical	Practise
1				The Shift Cipher and the Substitution Cipher	
2				The Affine Cipher, the Vigenere Cipher and the Hill Cipher	
3				The Permutation Cipher and the Stream Cipher	
4				Cryptanalysis of the Affine Cipher and Cryptanalysis of the Substitution Cipher	
5				Cryptanalysis of the Vigenere Cipher, Cryptanalysis of the Hill and Cryptanalysis of the LFSR Stream Cipher	
6				The Euclidean Algorithm and the Chinese Remainder Theorem	
7				Other Useful Facts and The RSA Cryptosystem	
8				Midterm Exam	
9				Legendre Symbols, Jacobi Symbols and the Solovay-Strassen Algorithm	
10				Miller-Rabin Algorithm and Square Roots Modulo n	
11				the Pollard p-1 Algorithm and the Pollard Rho Algorithm	
12				Dixon's Random Square Algorithm and Factoring Algorithms in Practice	
13				Computing Euler Phi function and the Decryption Exponent	
14				Wiener's Low Decryption Exponent Attack and the Rabin Cryptosystem	
15				Partial Information Concerning Plaintext Bits and Optimal Asymmetric Encryption Padding	

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
Final	1	2,00

Assesments

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

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

Table :

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

P.O. 2 : programcıktısı 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L.O. 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.

L.O. 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.

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