İ.Y.T.E

MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

LİSANSÜSTÜ PROGRAMLARINDA YENİ AÇILACAK

DERSLER İÇİN TANITIM FORMU

Gönderen : **Bilgisayar Mühendisliği Anabilim Dalı**

Bilgisayar Mühendisliği Yüksek Lisans Programı

Gönderilen : **Mühendislik ve Fen Bilimleri Enstitü Müdürlüğü**

Dersin Kodu ve Kredisi : CENG514 (3+0) 3

Dersin Adı (İngilizce) : Computational Number Theory

(Türkçe) : Bilgisayar Tabanlı Sayılar Teorisi

Dersin Amacı (İngilizce) : The aim of this course is to prepare the students for cryptography courses. Therefore the course is organized as "computational number theory". Upon completion of the course students are expected to develop skills to:
- understand the divisibility, prime numbers, congruencies, arithmetic with large integers, polynomial arithmetic, random numbers, and related theories.

(Türkçe) : Dersi alan öğrencilerin kriptografi derslerinde ve/veya bu amaçlı çalışmalarını yaparken sayılar kuramından ilgili kuramları biliyor ve kullanabiliyor olmalarının sağlanması amaçlanmaktadır.

Dersin İçeriği (İngilizce) : The course Schedule includes the mathematical theories, and tools which are importand for the cryptography such as the divisibility, prime numbers, congruencies, arithmetic with large integers, polynomial arithmetic, random numbers etc.

(Türkçe) : Ders içeriğinde sayılar kuramından bölünebilirlik, asal sayılar, büyük tamsayılarla modüler aritmetik gibi konularla ilgili kuramlar ve bu konuları kriptografi için önemli kılan yönleri incelenecektir.

Dersin Taslağı (İngilizce) :

1. Introduction to Computational Number Theory
2. Basic Properties of Integers; Divisibility, primality, GCD, LCM
3. Congruences ; Equivalence relations, Basic properties of congruencies, Linear congruencies, Chinese remainder theorem,

4. Congruences ;Residue classes, Euler Phi Function, Euler's Theorem and Fermat's Little Theorem, Quadratic residues, Summation over Division
5. Basic Integer Arithmetic, Computing in Zn, Faster Integer Arithmetic
6. Computation with large integers;
7. Asymptotic notation, Machine models and complexity theory,
8. Euclid's Algorithm; Basic and Extended Euclidean Algorithms, Computing Modular Inverses and Chinese Remaindering, Speeding up algorithms with modular computation
9. Prime Numbers; Distribution of prime numbers and primality testing
10. Abelian Groups ; Definitions and basic descriptions, Subgroups, Cosets and quotient groups, Group homomorphism and Isomorphism, Cyclic Groups
11. Rings; Definitions and basic descriptions, Polynomial Rings, Ideals and quotient rings, Ring homomorphism and isomorphism, Structure of Zn
12. Finite and Discrete Probability Distribution; Definitions, conditional probability and independence, Random variables, Expectation and variance,
13. Some useful bounds, Balls and bins, Hash Functions, Statistical Distance, Measures of Randomness, Discrete probability distribution
14. Probabilistic Algorithms; Definition and generating a random number from a given interval, Generate and test paradigm, Generating random prime

(Türkçe) :

1. Bilgisayar Tabanlı Sayılar Teorisine Giriş
2. Tamsayıların temel özellikleri: Bölünebilirlik, asallık, GCD, LCM
3. Moduler arithmetic ve ilgili kuramlar, özellikler.
    - Residue classes, Euler Phi Function, Euler's Theorem and Fermat's Little Theorem, Quadratic residues, Summation over Division
4. Moduler arithmetic ve ilgili kuramlar, özellikler.
    - Residue classes, Euler Phi Function, Euler's Theorem and Fermat's Little Theorem, Quadratic residues, Summation over Division
5. Temel tamsayı aritmetiği, Zn de hesaplamalar, Hızlı tamsayı aritmetiği
6. Büyük tam sayılarla arithemetik,
7. Asimtotik notasyon, makine modelleri ve karmaşa kuramı.
8. Euclid algoritmaları, modular Inverse ve Chinese Remaindering, modüler hesaplama ile algoritmaların hızlandırılması

9. Asal Sayılar; dağılışları, üretilmesi ve testleri
10. Abelian Grouplar; temel tanımlar, Subgroups, Cosets ve quotient groups, Group homomorphism ve Isomorphism, Cyclic Groups
11. Rings; temel tanımlar, Polynomial Rings, Ideals ve quotient rings, Ring homomorphism ve isomorphism, Zn yapısı
12. Sonlu ve ayrık olasılık dağılışı; tanımları, koşullu ve bağımsız olasılık, rastgele değişkenler, beklenen değer ve varyans,
13. Hash fonksiyonlar,istatiksel uzaklık, oluşturma ve test paradikması, rastgele asal sayıların oluşturulması.
14. Olasılık tabanlı algoritmalar.

Kullanılacak Materyal-Kitap ve Referanslar :

"A Computational Introduction to Number Theory and Algebra" book from http://shoup.net/ntb (Version 2)

A Friendly Introduction to Number Theory, Second Edition, Joseph H. Silverman

A Course in Number Theory and Cryptography, Second Edition, Neal Koblitz

A Course in Computational Number Theory, David Bressoud and Stan Wagon

The Art of Computer Programming, volume 2, Second edition, 1981, D. E. Knuth.

Değerlendirme Yöntemi :

Ara Sınav	%30
Dönem Projesi	%40
Final Sınavı	%30

Dersi Verecek Olan Öğretim Üyesi : Yrd. Doç. Dr. Serap ATAY