

SAKARYA ÜNİVERSİTESİ BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

**2023 KRİPTOLOJİ PROJESİ**

**ASAL SAYILAR İLE ANAHTAR ŞİFRELEME ALGORİTMASI TASARIMI**

İSİM SOYİSİM: FATMA GÜNER

ÖĞRENCİ NUMARASI: B201210373

SINIF: 1. ÖĞRETİM A GRUBU

**ASAL SAYILAR İLE ANAHTAR ŞİFRELEME ALGORİTMASI**

Bu proje, asal sayılar kullanılarak gerçekleştirilen bir anahtar kelime tabanlı şifreleme algoritmasını içermektedir. Algoritma, İngilizce alfabesi üzerinde çalışmakta olup, büyük harf ve Türkçe karakter girişlerini işleyebilmektedir. Şifreleme ve deşifre etme işlemleri sırasında asal sayılar, çözümü zorlaştıran bir özellik olarak kullanılmaktadır.

Girilen açık metindeki karakterler sırasıyla anahtar kelimedeki karakterler kullanılarak işlemlerden geçirilerek şifrelenmiş karakter elde edilir.

Eğer anahtar kelime, şifrelenecek metinden kısaysa anahtar kelimenin son karakterinden sonra ilk harfe geçerek bu şekilde şifrelenecek metindeki karakterler bitene kadar bu işlem devam eder.

Bu algoritmada ayrıca karakterin ASCII değerleri kullanılarak işlemler gerçekleşmektedir. Bu da algoritmanın çözülmesini zorlaştıran bir unsurdur.

Şifreli metni çözerken ise sadece şifreli metin ve gizli anahtar kullanılır.

metin, ekran görüntüsü, yazı tipi, diyagram içeren bir resim

Açıklama otomatik olarak oluşturuldu

**PROGRAMIN AMACI**

Bu programın temel amacı, asal anahtar şifreleme algoritması kullanarak metinleri güvenli bir şekilde şifrelemek ve şifreli metinleri orijinal hallerine geri çevirmektir. Asal sayılar, algoritmanın temel yapısını oluşturarak şifreleme işlemlerini daha karmaşık hale getirir ve bu da çözümü oldukça zorlaştırır. Anahtar kelimenin kullanımı, şifreleme sürecinde bir tür kılavuz görevi görerek güvenliği artırır.

Program, kullanıcıdan alınan metni belirli bir anahtar kelimeyle şifreleyerek, şifreli metni oluşturur. Şifreleme sürecinde her bir karakterin asal sayılarla yapılan matematiksel işlemlerle dönüştürülmesi, şifrenin güçlü ve tahmin edilmesi zor olmasını sağlar. Deşifre etme işlemi ise şifreli metinle kullanılan anahtar kelime sayesinde gerçekleştirilir. Bu sayede, sadece doğru anahtar kelimeye sahip olan kişilerin şifreli metni orijinal metne dönüştürme yeteneği bulunmaktadır.

Programın amacı, metin şifreleme işlemlerini güvenli ve karmaşık hale getirerek, verilerin güvenli bir şekilde iletilmesini veya depolanmasını sağlamaktır.

**Şifreleme:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Deşifreleme:** metin, ekran görüntüsü, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu