**T.C.**
**SAKARYA ÜNİVERSİTESİ**
**BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ**
**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

# BSM 465 KRİPTOLOJİYE GİRİŞ DERSİ PROJE RAPORU

# Şifreleme Algoritması Tasarımı

**HAZIRLAYANLAR**

**G201210036- Ayşe Esra AŞCI**
**B201210066- Hüsna ALTIN**

**Dersi Veren: Ünal ÇAVUŞOĞLU**

**2023-2024 Güz Dönemi**

Verilen proje ödevi kapsamında bizden güvenli iletişim ve veri koruma amaçlarıyla kullanılmak üzere yeni bir şifreleme algoritması tasarlamamız istenmiş olup projenin, temel şifreleme prensiplerini kullanarak bir blok şifreleme algoritması tasarımı ve performans ölçümleri üzerine odaklanması talep edilmiştir. Literatürdeki algoritmalardan esinlenerek yeni bir algoritma tasarımı yapmamız beklenmektedir. Ödevde istenen kriterler göz önüne alınarak proje oluşturulmuş olup proje oluşturulurken izlenen adımlar aşağıdaki gibidir.

**Projeye ait GitHub Linki:**https://github.com/husnaaltin/Kriptoloji

## 1.Literatür Taraması

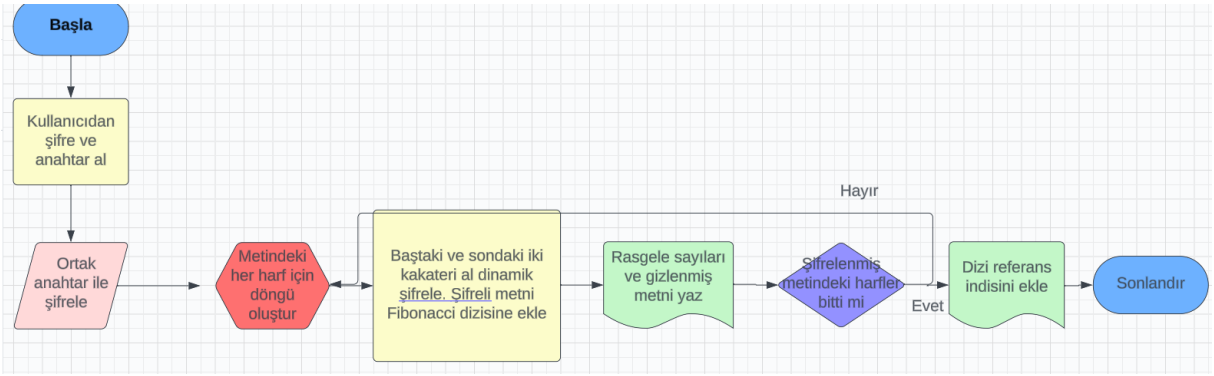
Ödeve başlarken ilk olarak fikir edinmek ve bilgi toplamak adına literatür taraması yapılmıştır. Şu anda ve geçmişte kullanılan popüler şifreleme algoritmaları araştırılmıştır. AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES), RSA (Rivest-Shamir-Adleman), Diffie-Hellman ve Caesar gibi şifreleme yöntemleri göz önünde bulundurulmuş ve çalışma mantıkları incelenmiştir. Ayrıca bu şifreleme algoritmalarından ilham alınarak oluşturulmuş farklı üniversitelerde bulunan öğrencilerin projeleri incelenmiştir. Nurettin TOPALOĞLU, M. Hanefi CALP ve Burak TÜRK' e ait "Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi" çalışması, Aysun COŞKUN ve Ülkü Ülker'e ait "Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti" adlı çalışma proje için bilgi toplama ve ilham verme konusunda yardım alınan kaynaklardan bazılarıdır. Bu çalışmalar incelenmiş ve projenin gerçekleştirilebilmesi için gereken bilgiler elde edildikten sonra bir sonraki adıma geçilmiştir.

## 2. Temel Prensiplerin Belirlenmesi

Çalışmamızda gönderici ve alıcı arasındaki iletişim, simetrik şifreleme tekniği kullanılarak gerçekleşir. Bu şifreleme algoritmasında asimetrik şifrelemenin aksine ortak bir tek anahtar vardır. Kullanıcıdan alınan mesaj şifrelenirken pi sayısının rakamlarının belli bir düzene veya örüntüye göre gitmeyip kendini tekrar etmemesinin oluşturduğu karmaşıklıktan ve Fibonacci dizisinin uyumundan yararlanılmıştır. Katmanlı bir mimariye sahip olan algoritma için sabit bir anahtar boyutu tanımlanmamıştır.

## 3. Algoritma Tasarımı

Şifreleme işlemimizde ilk olarak bilgi mesajı istenir. Mesaj harflere bölünür. Her harf için 5 haneli bir yer ayrılmaktadır. İlk 3 basamağı statik olarak, 4. ve 5. basamağı ise dinamik olarak verilir. Sayımızın 4. hanesini yazarken pi sayısından referans alınmıştır.

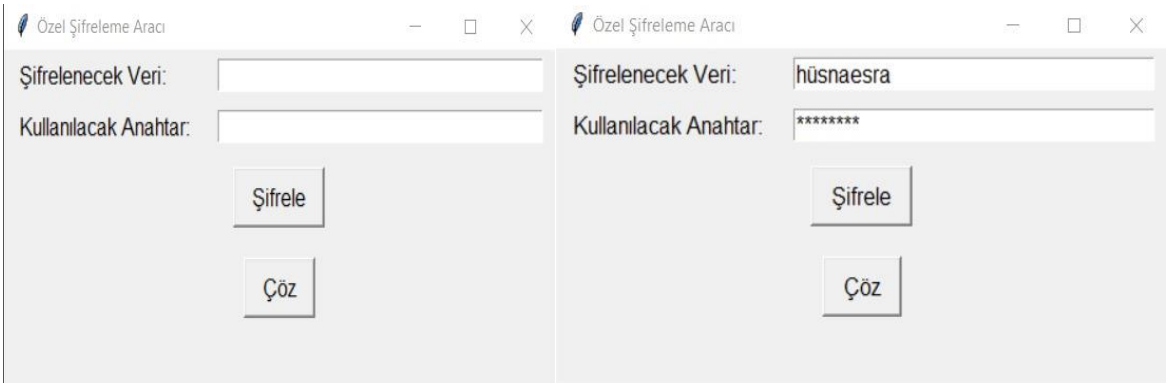


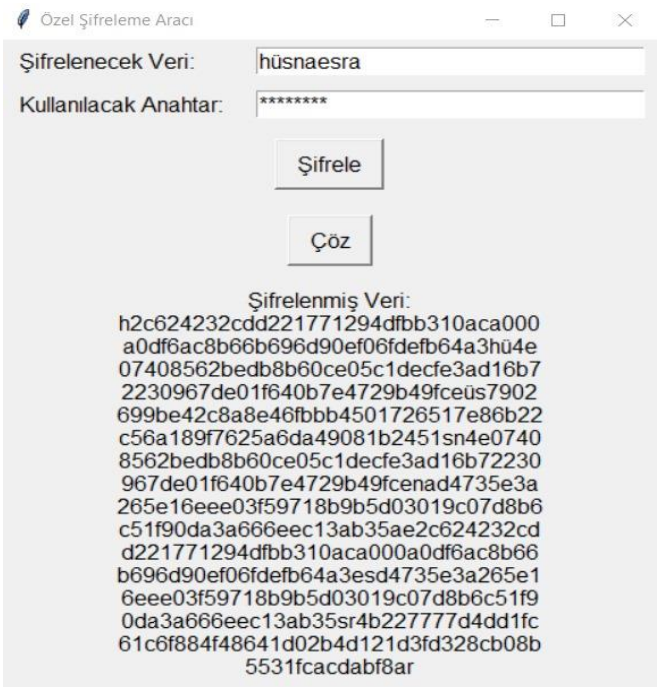

## 4. Anahtar Üretimi

Bu şifreleme algoritmasında asimetrik şifrelemenin aksine ortak bir tek anahtar vardır. Açık anahtarlı şifrelemede 2 çeşit anahtar mevcuttur. Genel Anahtar, orijinal verileri veya düz metni şifrelemek ve bir şifreli metin oluşturmak için kullanılır. Özel Anahtar ise oluşturulan bu şifreli metni çözümlemek için oluşturulmuştur. Algoritmanın hibrit çalışmasının birden fazla nedeni vardır.

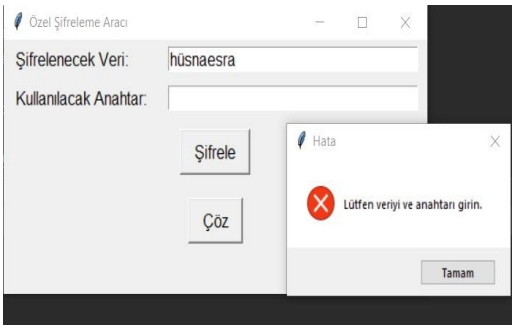
## 5. Algoritmanın Kodlanması

Proje Python dilinde PyCharm ortamında yazılmış olup şifrelenecek olan veri ve kullanılacak anahtarlar kullanıcıdan alınırken, şifreleme ve şifre çözme işlemi sonucu elde edilen sonuçlara ait ekran görüntüleri aşağıdaki gibidir.










Yukarıdaki görsellerde de görüldüğü gibi kullanıcıdan bir metin ve anahtar alınmakta şifrele butonuna basıldığında metin şifrelenerek ekrana basılmaktadır. Daha sonra çöz butonuna basıldığında ise tekrar orijinal metin ekrana basılmaktadır. Anahtar ve şifrelenecek metin alanı ise boş geçilememektedir.