BSG 9.HAFTA UYGULAMASI-ŞİFRELEME ALGORİTMASI

PROJE YÜRÜTÜCÜSÜ= Yunus Mert Bayat
ÖĞRENCİ-NO: 235542027

ŞUBE: Gündüz\A

1-) ALGORİTMANIN TANIMI:

1.1-) ALGORİTMANIN ADI: YMB (Yunus Mert Bayat) ALGORTİMASI.

1.2-) ALGORİTMANIN TİPİ: Akış şifreleme.

1.3-) ALGORİTMANIN TEMEL ALDIĞI İLKE: Collatz Conjecture(collatz sanısı).

1.4-) ALGORİTMANIN ÇALIŞMA MANTIĞI:

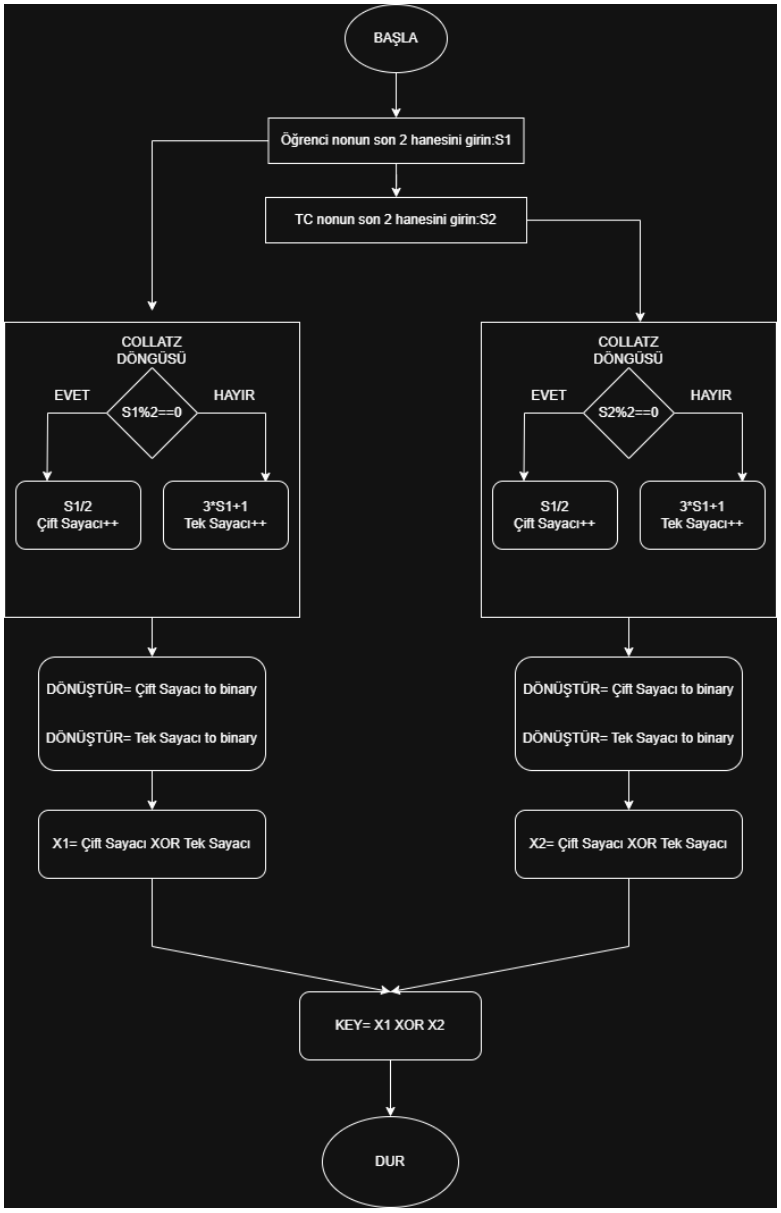
A-) Kullanıcıdan TC ve Öğrenci nosunun son 2 hanesi girdi olarak alınır.

B-) TC nosunun son 2 hanesi collatz conjecture e göre çözülür daha sonra çıkan sayı dizisindeki çift sayılar 0 tek sayılar ise 1 ile ifade edilir, son olarak tek sayıların toplamı ve çift sayıların toplamı binarye çevirilir(örneğin çift sayı adedi 0=5 ,binary karşılığı=101) ve bu binary sayılar kendi aralarında XORlanır.(örneğin: tek sayı adedinin binary karşılığı=101,çift sayı adedinin binary karşılığı=100, bu iki sayının XOR'u =001).

C-) B şıkkındaki tüm olay kullanıcın girdiği öğrenci nonun son 2 hanesi içinde uygulanır ve TC nodan çıkan XORlanmış binary sayı ile öğrenci nodan çıkan XORlanmış binary sayı kendi aralarında burda son kez XORlanır ve çıkan yeni binary değer bizim key (anahtarımız) olur.

D-) Son olarak kullanıcının şifrelemek istediği metin oluşturduğumuz key ile şifrelenir ve bu şifrelenmiş metni deşifrelemek istersek şifreli metni girdi olarak alıp düz metni elde edebiliriz.

E-) ALGORİTMANIN AKIŞ DİYAGRAMI:



2-) NEDEN BU TASARIM? :

2.1. Algoritma Tasarım Mantığı ve Güvenlik Analizi

Bu çalışmada önerilen şifreleme anahtarı üretim mekanizması, Collatz Sanısı'nın (3n+1 Problemi) kaotik doğasını temel almaktadır. Algoritmanın tasarımında aşağıdaki kriptografik prensipler gözetilmiştir:

2.1.1. Çığ Etkisi (Avalanche Effect) ve Hassasiyet

Collatz dizileri, başlangıç değerine karşı son derece hassastır. Birbirine yakın iki tam sayı (örneğin 26 ve 27), tamamen farklı uzunlukta ve karakterde diziler üretebilir. Bu durum, kriptografide aranan **"girdi üzerindeki küçük bir değişikliğin, çıktıda büyük ve öngörülemez bir fark yaratması"** kuralını sağlar. Böylece, kullanıcı verilerindeki (Öğrenci No/TC No) tek bir hanelik fark bile nihai şifrenin tamamen değişmesine yol açar.

2.1.2. Dinamik Entropi Kaynağı Olarak Collatz Dizileri

Algoritma, sayıların büyüklüğünden ziyade, bu sayıların 1'e ulaşana kadar geçtiği **yörünge karakteristiğini** (tek ve çift sayıların dağılımı) kullanır. Bu yöntem:

- Veri setini boyutsal olarak küçültürken, karakteristik bilgiyi korur.
- Statik bir anahtar yerine, matematiksel bir fonksiyonun çalışma süresinden (iterasyon sayısı) türetilen dinamik bir anahtar yapısı sunar.

2.1.3. Çok Katmanlı XOR Operasyonları ve Güvenlik Modeli

Tasarımda uygulanan çift katmanlı XOR (Özel Veya) mimarisi, iki bağımsız gizli değişkenin (Öğrenci ve TC No) etkileşimini sağlar.

1. **Birinci Katman (L1):** Her bir girdinin kendi içindeki parite (teklik-çiftlik) dengesi XOR'lanarak, o girdiye özgü bir "özet" (digest) çıkarılır.
2. **İkinci Katman (L2):** Elde edilen ara anahtarlar tekrar XOR'lanarak, değişkenler arasındaki korelasyon minimize edilir. Bu yapı, saldırganın girdilerden birine erişmesi durumunda bile diğer girdi üzerindeki belirsizliğin korunmasını sağlar.

2.1.4. Hesaplama Zorluğu ve Tersine Mühendislik Direnci

Collatz Sanısı'nın matematiksel olarak henüz genel bir formülle çözülememiş olması, algoritmanın tersine mühendisliğini zorlaştırır. Çıktıdan (final şifre) girdi değerlerine ulaşmak için sadece cebirsel işlemler yeterli olmayıp, her bir adımın simüle edilmesi gerekmektedir. Bu da brute-force (kaba kuvvet) saldırılarına karşı ek bir hesaplama maliyeti (computational cost) katmanı oluşturur.

3- MATEMATİKSEL FONKSİYONLAR:

A-) COLLATZ MATEMATİĞİ: Eğer kullanıcının girdiği sayı çift ise; n=n/2, kullanıcının girdiği sayı tek ise; n=3*n+1.

B-) XOR MANTIĞI: Akış şemasındada görüldüğü üzere önce kullanıcının girdiği her iki sayı kendi içinde çift ve tek sayılarının adedinin binary karşılığı oluşturulur ve binary(tek) ile binary(çift) aralarında XOR lanır ve X1 İLE X2 değişkenlerine atanır . Daha sonra bu X1 ve X2 değişkenleri kendi aralarında XORlanarak yeni key oluşturulur.

4-) ALGORİTMADAKİ KISITLAMALAR:

Algoritmanın zayıf karnı, 2^n formundaki girdilerdir. Bu sayılar doğrudan bölme işlemiyle hızla 1'e ulaştığı için düşük entropi üretir. Gelecek çalışmalarda, bu tür durumları engellemek için girdi değerlerine bir 'tuzlama' (salt) sabiti eklenmesi planlanmaktadır.

5-) ALGORİTMANIN KODA UYARLANMASI:

5.1-) KULLANILAN PROGRAMLAMA DİLİ: PYTHON

5.2-) KULLANILAN CODE BASE: VS CODE

6-) KODUN ÇIKTISI:

```
PS C:\Users\yunus> & C:/Users/yunus/AppData/Local/Programs/Python/Python39/python.ex
--- YMB (Collatz tabanlı) Şifreleme Sistemi ---
Öğrenci No (Son 2 hane): 27
TC No (Son 2 hane): 80
Şifrelenecek metni girin: YUNUS

[Sistem] Üretilen Anahtar: 102 (Binary: 1100110)
[+] Şifreli Metin: ?3(35
[+] Deşifre Edilen Metin: YUNUS

========================================
BİT DEĞİŞİMİ TESTİ (Anahtar 1 bit değişirse ne olur?)
Gerçek Key: 102 -> 0b1100110
Hatali Key: 103 -> 0b1100111
Hatali Key ile sonuç: XTOTR
========================================
PS C:\Users\yunus>
```