Collatz Conjecture Tabanlı Anahtar Üretimi ve Mesaj Şifreleme Sistemi

Özet

Bu çalışmada, matematikte çözülememiş problemlerden biri olan Collatz Conjecture kullanılarak deterministik ancak karmaşık bir anahtar (key) üretim yöntemi önerilmiştir. Üretilen anahtar, simetrik şifreleme yaklaşımıyla metin mesajlarının şifrelenmesi ve çözülmesinde kullanılmıştır. Çalışmanın amacı, matematiksel dizilerin kriptografik uygulamalarda kullanılabilirliğini incelemek ve alternatif anahtar üretim mekanizmaları geliştirmektir.

---

1. Giriş

Bilgi güvenliği, günümüzde dijital iletişimin temel yapı taşlarından biridir. Şifreleme yöntemleri, iletilen verinin yetkisiz kişiler tarafından okunmasını engellemek amacıyla kullanılmaktadır. Modern kriptografik sistemlerde anahtar üretimi, sistemin güvenliğini doğrudan etkileyen en kritik unsurlardan biridir.

Bu projede, matematiksel olarak basit tanımlanmasına rağmen oldukça karmaşık davranışlar sergileyen Collatz Conjecture kullanılarak bir anahtar üretim yöntemi tasarlanmıştır. Elde edilen anahtar, mesaj şifreleme sürecinde kullanılarak sistemin uygulanabilirliği gösterilmiştir.

---

2. Collatz Conjecture

Collatz Conjecture, pozitif bir tam sayıdan başlayan ve aşağıdaki kurallara göre ilerleyen bir sayı dizisini tanımlar:

- Eğer sayı çift ise: $n = n / 2$
- Eğer sayı tek ise: $n = 3n + 1$

Bu işlemler, sayı 1 olana kadar tekrarlanır. Henüz matematiksel olarak ispatlanmamış olmasına rağmen, denenmiş tüm pozitif tam sayılar için dizinin 1'e ulaştığı gözlemlenmiştir.

Collatz dizisinin düzensiz ve öngörülemez yapısı, bu çalışmada anahtar üretimi için bir avantaj olarak değerlendirilmiştir.

---

3. Sistem Tasarımı

3.1 Genel Mimari

Sistem üç temel aşamadan oluşmaktadır:

1. Collatz Conjecture kullanılarak bit dizisi üretimi
2. Üretilen diziden kriptografik anahtar oluşturulması
3. Anahtar kullanılarak mesaj şifreleme ve çözme işlemi

Bu aşamalar sırasıyla ve deterministik bir biçimde çalışmaktadır.

---

4. Anahtar Üretim Yöntemi

4.1 Seed (Başlangıç Değeri)

Anahtar üretim süreci, gizli bir başlangıç sayısı (seed) ile başlar. Bu sayı, sistemin güvenliği açısından gizli tutulmalıdır. Aynı seed kullanıldığında her zaman aynı anahtar üretilmektedir.

4.2 Bit Dizisi Oluşturma

Collatz adımlarında elde edilen sayıların tek veya çift olma durumuna göre bitler üretilmiştir:

- Tek sayı → 1
- Çift sayı → 0

Bu şekilde elde edilen bit dizisi, belirlenen uzunluğa ulaşana kadar üretilmeye devam eder.

4.3 Hash ile Güçlendirme

Doğrudan elde edilen bit dizisinin kriptografik olarak yeterince güçlü olmaması ihtimaline karşı, Collatz çıktısı SHA-256 hash algoritması ile işlenmiştir. Bu işlem sonucunda sabit uzunlukta ve daha yüksek entropiye sahip bir anahtar elde edilmiştir.

---

5. Mesaj Şifreleme Yöntemi

5.1 Metin – Binary Dönüşümü

Şifrelenecek mesaj, ASCII tabanlı olarak binary (ikili) forma dönüştürülmüştür. Her karakter 8 bit ile temsil edilmiştir.

5.2 XOR Tabanlı Şifreleme

Şifreleme işlemi XOR (özel veya) mantıksal işlemi kullanılarak gerçekleştirilmiştir. XOR işleminin simetrik yapısı sayesinde aynı anahtar ile hem şifreleme hem de çözme işlemi yapılabilmektedir.

Şifreleme işlemi şu şekilde özetlenebilir:

- Mesaj bitleri ile anahtar bitleri XOR işlemine tabi tutulur
- Elde edilen çıktı şifreli mesajı oluşturur

---

6. Deşifreleme Süreci

Deşifreleme işlemi, şifreleme ile aynı adımları izlemektedir. Şifreli mesaj, aynı anahtar ile tekrar XOR işlemine sokularak orijinal mesaja geri dönüştürülmektedir.

Bu özellik, sistemin simetrik şifreleme prensibine dayandığını göstermektedir.

---

7. Güvenlik Değerlendirmesi

7.1 Avantajlar

- Collatz Conjecture deterministik ancak karmaşık bir yapı sunar

- Seed bilinmeden anahtar üretilemez
- Hash algoritması ile anahtar güçlendirilmiştir

7.2 Sınırlamalar

- Collatz Conjecture kriptografik olarak kanıtlanmış bir rastgelelik kaynağı değildir
- XOR tek başına güçlü bir şifreleme yöntemi değildir
- Gerçek dünya uygulamalarında AES gibi standart algoritmalarla desteklenmelidir

---

8. Sonuç

Bu çalışmada, Collatz Conjecture kullanılarak alternatif bir anahtar üretim yöntemi geliştirilmiş ve bu anahtar ile mesaj şifreleme işlemi gerçekleştirilmiştir. Elde edilen sonuçlar, matematiksel dizilerin kriptografi alanında deneysel ve eğitim amaçlı olarak kullanılabileceğini göstermektedir.

Gelecek çalışmalarda, önerilen anahtar üretim yönteminin daha gelişmiş şifreleme algoritmalarıyla birlikte kullanılması ve istatistiksel analizlerle değerlendirilmesi planlanmaktadır.

---

9. Kaynakça

1. Lagarias, J. C. (2010). *The 3x+1 Problem: An Annotated Bibliography*.
2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*.
3. Schneier, B. (1996). *Applied Cryptography*.


```
PS C:\Users\TUĞBA\OneDrive\Masaüstü\bsg final proje> & C:/Users/TUĞBA/AppData/Local/Programs/Python/Python314/python.exe "c:/Users/TUĞBA/OneDrive/
Masaüstü/bsg final proje/bsgfinalproject.py"
Orijinal Mesaj: MERHABA
Üretilen Key (ilk 64 bit): 0000110100110110010111001001111101100000011010011010001001101111
Şifreli Mesaj (binary): 0100000001110011000011101101011100100001001010111110011
Çözülen Mesaj: MERHABA
PS C:\Users\TUĞBA\OneDrive\Masaüstü\bsg final proje>
```