

BAŞLIK: Chaos-Shuffle Algoritması Sözde Kod (Pseudocode) ve Teknik Açıklama

1. Girdi ve Çıktı Tanımları

- **Girdi (Input):**
 - **seed**: 15 haneli pozitif tam sayı (Başlangıç entropisi).
 - **length**: Üretilmesi istenen bit uzunluğu.
- **Çıktı (Output):**
 - **bits**: 0 ve 1'lerden oluşan dizi.

2. Kullanılan Değişkenler

- **State (S)**: 64-bit İşaretsiz Tam Sayı (Hafıza).
- **Chaos (X)**: Çift hassasiyetli reel sayı (Kaotik motor).
- **Mu**: 3.99995 (Kaotik katsayı sabiti).
- **Mask**: 8-bitlik geçici karıştırma değeri.

3. Sözde Kod (Pseudocode)

Plaintext

FONKSİYON ChaosShuffle_Gen (seed, length)

// BAŞLATMA EVRESİ

S = seed VE (2⁶⁴ - 1) // 64-bit maskeleme

X = (seed MOD 10⁷) / 10⁷

EĞER X == 0 İSE: X = 0.123456

Bits_Listesi = []

// ÜRETİM DÖNGÜSÜ

DÖNGÜ i'den length'e KADAR:

// Adım 1: Kaotik Lojistik Harita

X = 3.99995 * X * (1.0 - X)

// Adım 2: Dinamik Maske Türetimi

Maske = TAMSAYI(X * 10¹²) VE 0xFF

// Adım 3: Karıştırma (XOR)

S = S XOR (Maske SOLA_KAYDIR 56)

// Adım 4: Difüzyon (19-Bit Rotasyon)

Sol_Parca = S SOLA_KAYDIR 19

Sag_Parca = S SAĞA_KAYDIR 45

S = (Sol_Parca VEYA Sag_Parca) VE (2⁶⁴ - 1)

// Adım 5: Döngü Kırıcı (Opsiyonel Güvenlik)

EĞER S < 1000 İSE:

S = S XOR TAMSAYI($X * 10^{15}$)

// Adım 6: Çıktı Süzme (LSB)

Bit = S VE 1

Bits_Listesi.EKLE(Bit)

DÖNGÜ SONU

DÖNDÜR Bits_Listesi

FONKSİYON SONU