Chaos-Logistic-RNG: Proje Raporu

Ders: Bilgi Sistemleri ve Güvenliği

Konu: Rastgele Sayı Üreteci (RSÜ) Tasarımı ve Analizi

BÖLÜM 1: ALGORİTMA MANTIĞI VE ÇALIŞMA PRENSİBİ

1.1. Temel Felsefe

Bu proje, rastgele sayı üretiminde geleneksel lineer yöntemler yerine, **Kaos Teorisi**'nin temel taşlarından biri olan **Lojistik Harita (Logistic Map)** denklemini temel almaktadır. Algoritma, kaotik sistemlerin başlangıç koşullarına olan aşırı hassasiyetini (Kelebek Etkisi) kullanarak, tahmin edilmesi imkansız bit dizileri üretmeyi hedefler.

1.2. Matematiksel Model

Algoritma şu lineer olmayan fark denklemi üzerine kuruludur:

x(n+1) = r * x(n) * (1 - x(n))

Burada kullanılan parametreler şunlardır:

- **r (Kaos Katsayısı):** Sistemin kaotik davranış sergilemesi ve periyodik döngülere girmemesi için r değeri **3.999999** olarak seçilmiştir.
- **x0 (Tohum/Seed):** Sistemin başlangıç değeri, bilgisayarın o anki sistem zamanının (System Time) mikrosaniye hassasiyetindeki ondalık kısmından alınır. Bu sayede algoritma her çalıştırıldığında benzersiz bir başlangıç noktasına sahip olur.

1.3. Bit Üretim Süreci (Extraction)

Denklem sonucunda elde edilen x değeri sürekli 0 ile 1 arasında değişen ondalıklı bir sayıdır. Virgülden sonraki basamaklar, kaos teorisi gereği yüksek entropiye (rastgeleliğe) sahiptir. Algoritma şu adımları izler:

1. **İterasyon:** Denklem işletilerek yeni x değeri bulunur.
2. **Genişletme:** Virgülden sonraki karmaşayı yakalamak için x değeri 10 üzeri 14 (10^14) ile çarpılarak tam sayıya dönüştürülür.
3. **Modülo İşlemi:** Elde edilen tam sayının 2'ye göre modu alınarak (Mod 2) sonuç **0** veya **1** bitine dönüştürülür.

BÖLÜM 2: ALGORİTMA ÇIKTILARI VE TEST SONUÇLARI

Aşağıdaki blok, algoritmanın 2000 bitlik üretimi sonucunda elde edilen verileri ve NIST standartlarına uygun istatistiksel test sonuçlarını (Frekans, Ki-Kare ve Runs testleri) göstermektedir.

```
>>> SİSTEM BAŞLATILIYOR: Chaos-Logistic-RNG v1.0
>>> Yöntem: Kaos Teorisi / Lojistik Harita Dönüşümü

>>> 2000 adet rastgele bit üretiliyor... Lütfen bekleyiniz.
>>> Üretim Tamamlandı. Süre: 0.0008 saniye.

Örnek Çıktı (İlk 64 Bit):
[1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0,
```

```
   ============================================================
   TEST 1: FREKANS (MONOBIT) ANALİZİ
   ============================================================
   [-] Toplam Bit Sayısı : 2000
   [-] 0 Sayısı (Zeros)  : 1037 (Oran: %51.8500)
   [-] 1 Sayısı (Ones)   : 963  (Oran: %48.1500)
   [-] Fark (Delta)      : 74

   ============================================================
   TEST 2: Kİ-KARE (CHI-SQUARE) UYUMLULUK TESTİ
   ============================================================
   [-] Hesaplanan X² Değeri : 2.7380
   [-] Kritik Eşik Değer    : 3.841 (p=0.05)
   [+] SONUÇ: BAŞARILI ✅
       (X² < 3.841 olduğu için H0 hipotezi kabul edildi.
       Dağılım istatistiksel olarak rastgele kabul edilebilir.)

   ============================================================
   TEST 3: KOŞU (RUNS) TESTİ (Bağımsızlık Analizi)
   ============================================================
   [-] Gözlenen Koşu Sayısı : 1010
   [-] Beklenen Koşu Sayısı : 999.6310
   [-] Standart Sapma       : 22.3245
   [-] Z-Skoru (Z-Score)    : 0.4645
   [+] SONUÇ: BAŞARILI ✅
       (Z-Skoru ±1.96 aralığında. Bitlerin dizilimi bağımsızdır.)
```