T.C.

Fırat Üniversitesi

Yazılım Mühendisliği Bölümü

**YAZILIM MÜHENDİSİLİĞİ GÜNCEL KONULAR DERSİ GÜVENLİ DİJİTAL HAYAT PROJESİ DOKÜMANTASYONU**

**Eyüp Ensar KASAP**

**HAZİRAN-2022**

İçindekiler

[Şekiller listesi 2](#_Toc105947230)

[1. GİRİŞ 3](#_Toc105947231)

[1.1. Mersenne Twister 3](#_Toc105947232)

[1.2. NIST(istatistiksel test süiti) 3](#_Toc105947233)

[2. MATERYAL VE METOT 4](#_Toc105947234)

[2.1. Rastgele Sayı Üretecinin Geliştirilmesi 4](#_Toc105947235)

[2.1.1. Visual Studio IDE 4](#_Toc105947236)

[2.1.2. StreamWriter sınıfı 4](#_Toc105947237)

[2.2. Rastgele sayı üreteci ile 1.000.000 – bit üretme işlemi 4](#_Toc105947238)

[2.3. ÜRETİLEN 1.000.000 – BİTENIST TESTİ UYGULANMASI 5](#_Toc105947239)

[3. BULGULAR TARTIŞMA 6](#_Toc105947240)

[4. SONUÇ 8](#_Toc105947241)

# Şekiller listesi

[Şekil 2.1 Rastgele sayı üreteci ile 1.000.000 – bit üretme işlemi 4](#_Toc105947275)

[Şekil 2.2 Üretilen 1.000.000 – bit .txt dosyası görseli 5](#_Toc105947276)

[Şekil 2.2.1 Üretilen 1.000.000 – bit .txt dosyası görseli 2 5](#_Toc105947276)

[Şekil 2.3 NIST testi Uygulanması 5](#_Toc105947277)

[Şekil 2.4 NIST test sonuçları 6](#_Toc105947278)

# Tablolar listesi

[Tablo 2.1 NIST test sonuçları 6](#_Toc105947254)

[Tablo 2.2 NIST test sonucu P değerleri 7](#_Toc105947255)

# GİRİŞ

Proje kapsamında C# dili ve Mersenne Twister algoritması ile 1 milyon bit üretilmiştir. Üretilen bitlerin kaydı alınarak NIST(istatistiksel test süiti) testinden geçirilmiştir.

## Mersenne Twister

**Mersenne Twister**, 1997 yılında [Makoto Matsumoto](https://en.wikipedia.org/w/index.php?title=Makoto_Matsumoto&action=edit&redlink=1" \o "Makoto Matsumoto (page does not exist))ve [Takuji Nishimura](https://en.wikipedia.org/w/index.php?title=Takuji_Nishimura&action=edit&redlink=1" \o "Takuji Nishimura (page does not exist))tarafından geliştirilen genel amaçlı bir [sözde rasgele sayı üretecidir](https://en.wikipedia.org/wiki/Pseudorandom_number_generator) (PRNG) . [[1]](https://en.wikipedia.org/wiki/Mersenne_Twister#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Mersenne_Twister#cite_note-2)[Adı, periyod uzunluğunun bir Mersenne asal](https://en.wikipedia.org/wiki/Mersenne_prime) olarak seçilmesi gerçeğinden gelmektedir.  
 Mersenne Twister, özellikle eski PRNG'lerde bulunan kusurların çoğunu düzeltmek için tasarlandı.  
Mersenne Twister algoritmasının en yaygın kullanılan versiyonu, Mersenne asal algoritmasına dayanmaktadır{\ Displaystyle 2^{19937}-1}. Bunun standart uygulaması olan MT19937, [32 bitlik](https://en.wikipedia.org/wiki/32-bit) bir kelime uzunluğu kullanır. 64 bitlik bir sözcük uzunluğu kullanan başka bir uygulama (beş değişkenli [[3] ) vardır, MT19937-64;](https://en.wikipedia.org/wiki/Mersenne_Twister#cite_note-3)farklı bir dizi oluşturur.

Avantajları;

* Mevcut çeşitli jeneratörlerin kusurları dikkate alınarak tasarlanmıştır.
* Algoritma aşağıda indirilebilir bir C kaynağına kodlanmıştır.
* Uygulanan diğer herhangi bir üreticiden çok daha uzun süre ve çok daha yüksek bir eşitlik dağılımı. (Periyodun 2^19937-1 olduğu kanıtlanmıştır ve 623 boyutlu eşit dağılım özelliğinin sağlandığı garanti edilmiştir.)
* Hızlı nesil. (Sisteme bağlı olsa da, boru hattı ve önbellek içeren bir sistemde MT'nin bazen standart ANSI-C kitaplığından daha hızlı olduğu bildirilir.) (2004/3'te eklenen not: 1998'de, genellikle MT'nin şundan çok daha hızlı olduğu bildirilir. Rand(), ancak Rand() algoritması değiştirildi ve şimdi hızda fazla bir fark yok.)
* Belleğin verimli kullanımı. (Uygulanan C kodu mt19937.c yalnızca 624 kelimelik çalışma alanı tüketir.)

NIST(istatistiksel test süiti)

* NIST istatistiksel test süiti hipotez test tabanlı bir test türüdür.
* Bu hipotez testler üretilen 0 veya 1 sayısının rastgele olup olmadığını belirler.
* Bu amaç için NIST test süitinde iki önemli parametre vardır bunlar sırasıyla α ve P-Değeri değeridir.
* Önem seviyesi olarak bilinen α ‘nın 0.01 olarak seçilmesi test edilecek sayıların rastgeleliğinin 99% güven değerine sahip olduğunu belirtir.
* Diğer parametre P-değeri rastgeleliğin ölçüsü olarak bilinir. Eğer P-değeri 1’e eşit olursa sayılar mükemmel rastgeleliğe sahiptir denir.
* P-değeri sıfıra eşit olursa sayıların rastgeliğinden söz edilemez.
* Kriptografik uygulamalarda kullanılmak üzere üretilen sayıların önem seviyesi α, uygun bir değer seçilmelidir.
* Her bir test için eğer P-değeri, α değerinden büyük ve eşit olursa test başarılıdır. Aksi durumda test başarısız yani üretilen sayılar rastgele değildir. Genellikle önem seviyesi [0.001, 0.01] aralığında seçilir.
* NIST testi güçlü bir testtir ve bu nedenle kriptografik uygulamalarda tercih edilmektedir.
* Rastgele sayı üreteçleri tarafından üretilen uzun ikili bit dizilerinin rastgeleliğini ölçmek için geliştirilmiştir.
* NIST 800-22 kendi içinde 15 tane ayrı testten oluşur.
* Teste tabi tutulan bit dizisinin başarılı olabilmesi için tüm testleri başarıyla geçmesi gerekmektedir.
* Bu testler dizi içerisindeki rastgele olmayan durumlara odaklanır.

# MATERYAL VE METOT

Bu proje de Mersenne Twister yani rastgele üreteci Microsoft’ un Visual Studio uygulaması kullanılmıştır. Kullanılan dil C#’ tır. NIST testinin uygulanması için de Random Numbers Analyser uygulaması kullanılmıştır.

## Rastgele Sayı Üretecinin Geliştirilmesi

Mersenne Twister algoritması ve C# dili kullanılarak üretilen rastgele sayı üreteci ile 1.000.000 – bit elde edilmiştir. Elde edilen bitler “System.IO” kütüphanesinin “StreamWriter” sınıfı kullanılarak “.txt” uzantılı dosyaya çıktı olarak aktarılmıştır.

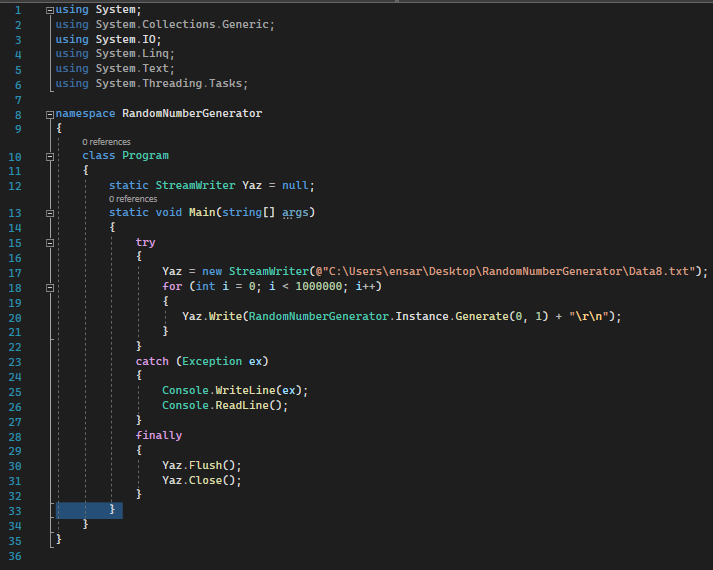
## Visual Studio IDE

Microsoft Visual Studio, Microsoft tarafından geliştirilen bir tümleşik geliştirme ortamıdır.

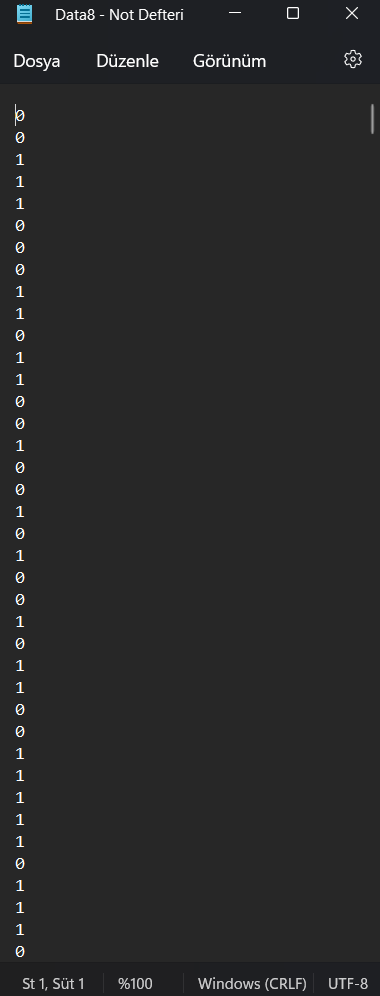
## StreamWriter sınıfı

StreamWriter sınıfında System.IO kütüphanesi kullanılır. Bu sınıfın temel amacı metin dosyalarına karakter girişi sağlamaktır. Bilgisayar üzerinde bulunan bir dosyaya StreamWriter sınıfıyla erişilir ve bu dosyaya karakter girişi sağlanır.

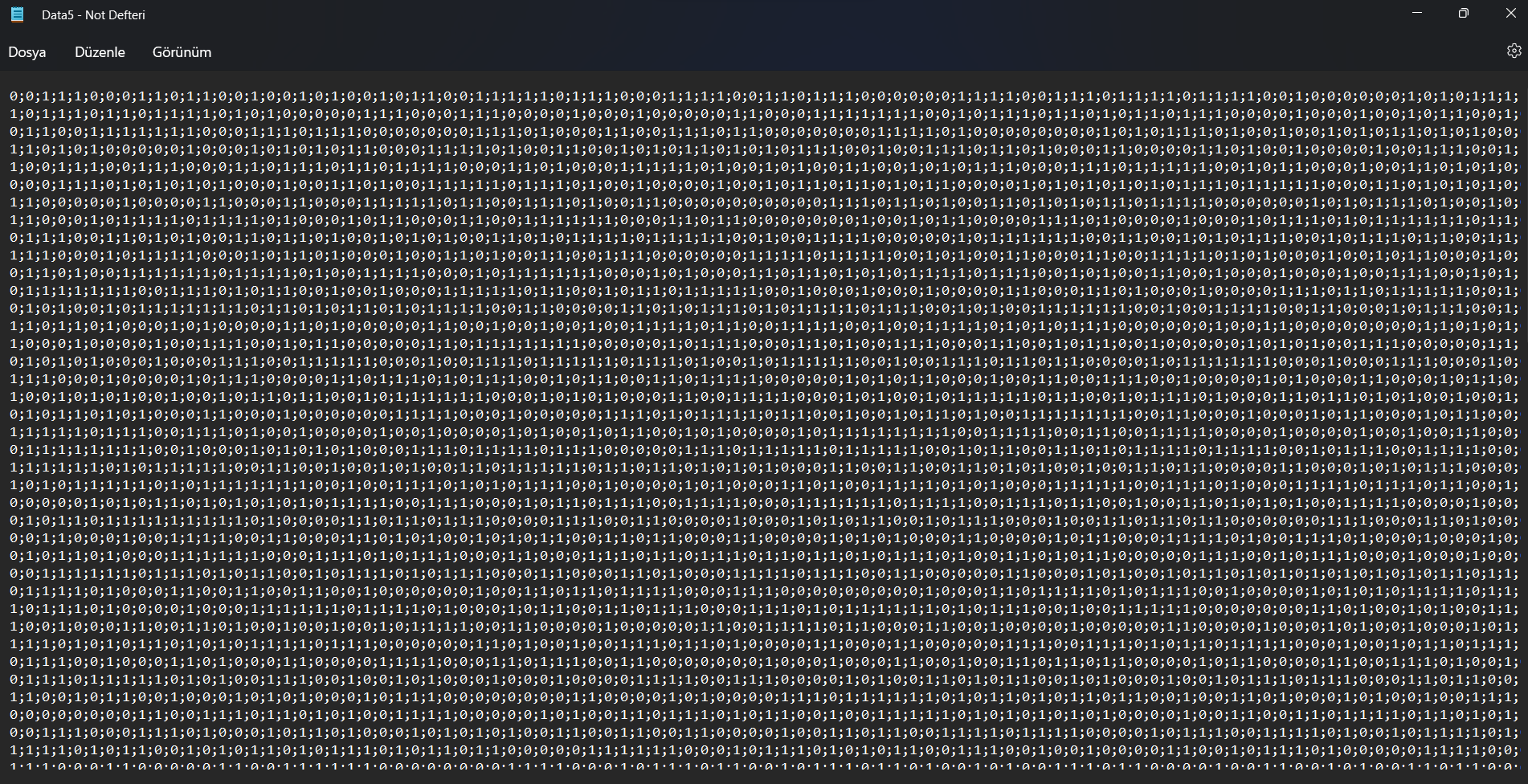
## Rastgele sayı üreteci ile 1.000.000 – bit üretme işlemi



Şekil 2.1 Rastgele sayı üreteci ile 1.000.000 – bit üretme işlemi

****

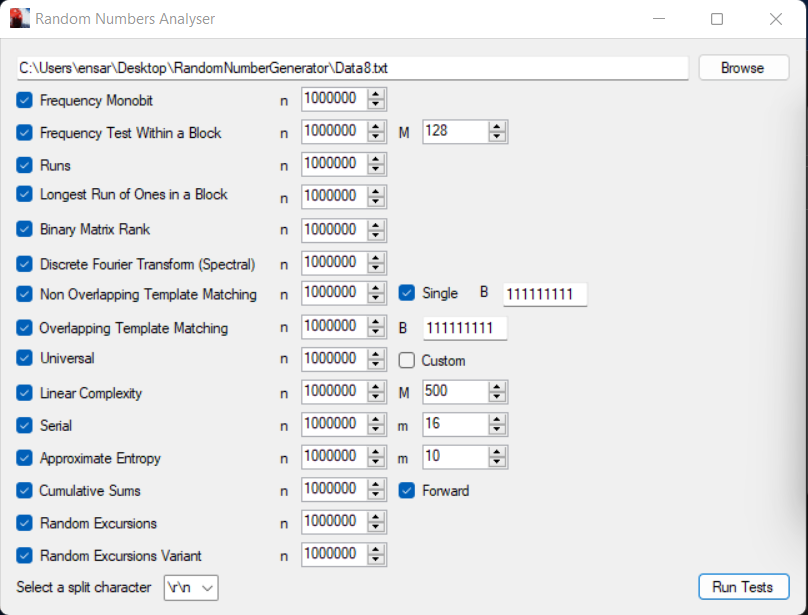
Şekil 2.2 Üretilen 1.000.000 – bit Data8.txt dosyası görseli



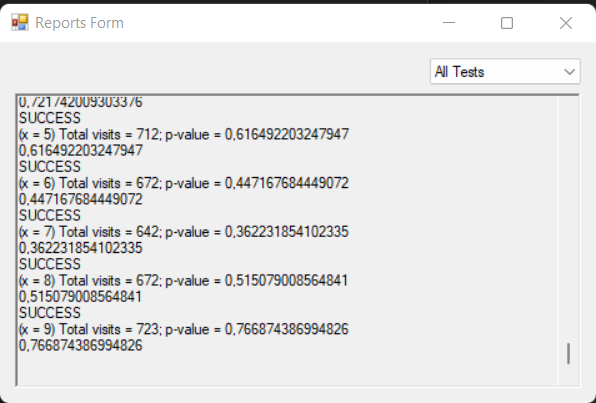
Şekil 2.2.1 Üretilen 1.000.000 – bit Data8.txt dosyası görseli 2

## Üretilen 1.000.000 – Bite NIST Testi Uygulaması

.txt uzantıı dosyanın yolu Random Numbers Analyser programında seçilerek uygulanacak NIST testleri belirlendikten sonra “Run Tests” denilerek test işlemi gerçekleştirilmiştir.



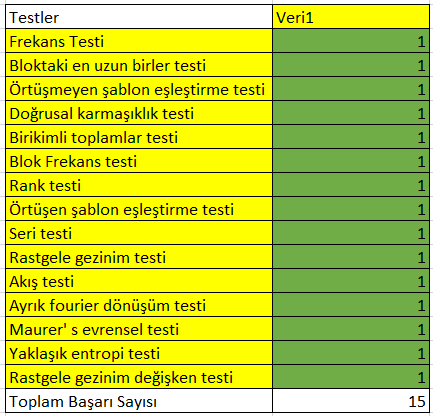
Şekil 2.3 NIST testi Uygulanması



Şekil 2.4 NIST test sonuçları

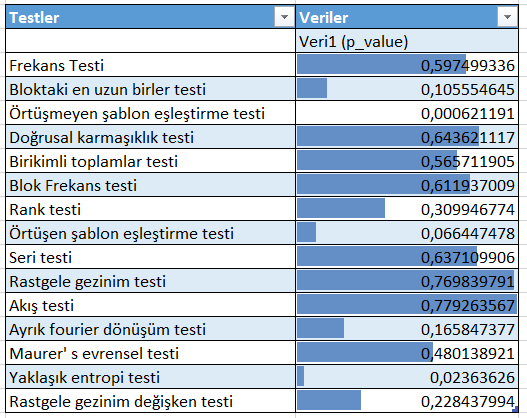
# BULGULAR TARTIŞMA

1. Tablo 3.1 NIST test sonuçları



1’ er milyonluk veri setinin NIST test sonuçları Tablo 2.1 de gösterilmektedir.

Tablo 3.2 NIST test sonucu P değerleri



Elde edilen P değerleri önem değeri olan 0,01‘ den büyük olduğu için testleri başarıyla geçmiştir.

# SONUÇ

Tüm testleri başarılı olarak tamamlayan veri setlerinin rastgele olduğu kanıtlanmış olup verilerin güvenliği için şifreleme algoritmalarında anahtar olarak kullanılabileceği sonucuna ulaşılmıştır.