



T.C.
SAKARYA ÜNİVERSİTESİ

BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
PROGRAMLAMA DİLLERİNİN PRENSİPLERİ ÖDEV RAPORU

Rastgele Karakter Üretimi

Grup Elemanları:

G141210402 - Furkan Hasan SAKACI (2A)

SAKARYA

Mart, 2019

Rastgele Karakter Üretimi

Furkan Hasan SAKACI

G141210402 – 2A

Özet

Kriptoloji çalışmalarının daha başarılı olabilmesi için rastgele karakter üretiminde rastgeleliğin sağlanmasıdır. Bunun için farklı yöntemler kullanılsa da rastgeleliği sağlayan en önemli yöntem sistemin mikro saniyelerden düşük çalışma zamanıdır. Çalışma zamanını kullanarak rastgele karakter üretmek için mod ve toplama işlemi kullanılabilir. Burada mod işlemi aralık farkını toplama işlemi ise bu aralığın kaçtan başlayacağını belirtmektedir. Burada yapılan çalışma da nano saniyeler kullanılarak karakter üretimi yapılmıştır. Burada farklı fonksiyonlar için mod aralığı değiştirilerek farklı fonksiyonlar oluşturulmuştur. Literatürde bu tür çalışmalar yapılmış olup genel olarak bu çalışmalar da hazır random kütüphanesi kullanılmıştır. Kelime ve cümle üretmek için ise bu karakterler birleştirilmiştir. Daha sonra bu kelime ve cümleler test dosyası kullanılarak test edilmiştir.

© 2017 Sakarya Üniversitesi.

Bu rapor benim özgün çalışmamdır. Faydalanmış olduğum kaynakları içerisinde belirttim. Her hangi bir kopya işleminde sorumluluk bana aittir.

Anahtar Kelimeler: Rastgele karakter, kriptoloji, kriptanaliz, kriptolama.

1. GELİŞTİRİLEN YAZILIM

Yapılan çalışma da nano saniyeler kullanılarak kelime ve cümle üretebilen kütüphane hazırlanmıştır. Burada oluşturulan kütüphanenin fonksiyonları tablo 1 ile verilmiştir.

Tablo 1. Fonksiyonlar

Fonksiyon İsmi	Giriş Parametresi	Çıkış Parametresi
AdetKarakterUret	int adet	Char[]
CumleUret	int kelime adeti	String
KarakterArasıUret	char bas, char son	String
KaraktereGoreUret	char[]	Char[]

Yapılan kütüphanenin testi yapıldıktan sonra elde edilen sonuçlar şekil 1 ile verilmiştir.

```
run:
Rastgele 100 karakter: hoqkkfCkjWwkspalJBfkaOKvoNikUrCvTQfVYxTWGjQPvJrcBRpOHTWVUI
Rastgele cümle: CsLBYyDEnNbKupSeLp UTKimPF gLOgJtTOuShJLpComp tLJyPqwukUTpKQFMC j
a ve h karakterleri arası: hcdhadbagahdahcbhfh
a, b, f, h, t, c ve s karakterlerinden kelime: bschahbfhafttas
BUILD SUCCESSFUL (total time: 1 second)
|
```

Şekil 1. Test sonucu

2. ÇIKTILAR

Yapılan çalışma sonucunda istenen sayıda kelime ve karakter üretimi rastgele yapabilmektedir.

3. SONUÇ

Yapılan çalışma sayesinde kriptoloji alanında rastgelelik sağlanarak bu alanda yapılacak çalışmalara öncülük edecektir.

Referanslar

- [1] <https://en.wikipedia.org/wiki/Nanosecond>
- [2] A.Adin., The analysis of random amplitude nanosecond pulses, Israel Atomic Energy Commission, Tel-Aviv, Israel, Received 25 April 1968, Available online 30 October 2002.