T.C.

SAKARYA ÜNİVERSİTESİ

BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

PROGRAMLAMA DİLLERİNİN PRENSİPLERİ ÖDEV RAPORU

Kriptolama İşlemleri İçin Rastgele Karakter Üretimi

Grup Elemanları:

B141210407 – Emine ÇETİNER (1C)

SAKARYA

Mart, 2019

Programlama Dillerinin Prensipleri Dersi

Kriptolama İşlemleri İçin Rastgele Karakter Üretimi

Emine ÇETİNER

B141210407 – 1C

Özet

Kriptoloji de en önemli unsurlardan biri rastgele karakter üretimidir. Herhangi bir sayının bir parametreye bağlı olması rastgeleliği azaltması ve bu nedenle kriptolanan yapıların çözülmesine neden olmaktadır. Bunun için farklı yöntemler kullanılsa da rastgeleliği sağlayan en önemli yöntem sistemin mikro saniyelerden düşük çalışma zamanıdır. Çalışma zamanı belirli matematiksel işlemlerden geçirilerek istenilen aralıkta rastgele karakter üretimi için kullanılabilmektedir. Burada yapılan çalışma da nano saniyeler kullanılarak karakter üretimi yapılmıştır. Literatürde bu tür çalışmalar yapılmış olup genel olarak bu çalışmalar da hazır random kütüphanesi kullanılmıştır. Kelime ve cümle üretmek için ise bu karakterler birleştirilmiş ve oluşturulmuş yapıların rastgeleliği test dosyası kullanılarak test edilmiştir.

© 2017 Sakarya Üniversitesi.
Bu rapor benim özgün çalışmamdır. Faydalanmış olduğum kaynakları içeresinde belirttim. Her hangi bir kopya işleminde sorumluluk bana aittir.

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

1. GELİŞTİRİLEN YAZILIM

Yapılan çalışma da öncelikle oluşturulmuş kütüphanenin fonksiyonlar tablo 1 ile verilmiştir. Burada görüldüğü üzere karakter, kelime ve cümle fonksiyonları birbirinden ayrıdır.

Tablo 1. Fonksiyonlar

Fonksiyon İsmi	Giriş Parametresi	Çıkış Parametresi
GenarateChar	-	Char
GenerateVocabulary	int count	String
GenerateSentence	int count	String
GenerateBetween	char start,char end, int count	String
GenarateSelect	String Characters, int count	String

Yapılan kütüphanede öncelikle tek bir karakter üretme fonksiyonu oluşturulmuştur. Daha sonra kelime üretmek için üretilecek kelimenin uzunluğu fonksiyona verilerek bir döngü içerisinde tek tek karakter üretme fonksiyonundan gelen değerler çekilmiştir. Aynı şekilde cümle üretme işlemi ise 3 ile 13 arasında rastgele

kelimelerden oluşan ve kelime adetini dışarıdan alan bir fonksiyondur. Bunların dışında belirli aralıkta ve belirli karakterlere göre üretim yapan fonksiyonlar ise oluşturulacak kelimenin uzunluğunu dışarıdan almaktadır. Oluşturulmuş kütüphanenin testi yapıldığında oluşan çıktı şekil 1 ile verilmiştir.

```
Tek karakter üret: y
100 karakter üret: kJveTKlsGqsmTmKxIPiNlFellomkYADhPbuwbwrMLRHaLlrhpFbruUiiAJcActCTruSmwjmQTINhvJfkWO
5 kelimeli cümle üret(her kelime 3 ile 13 arasında rastgele): AGmUMDvufd cDOadN mSbNl DFAttjvPkicQ rR
a ile h arasında 5 karakterli kelime üret: ffgae
asdczflu karakterlerinden 10 karakterli kelime üret: azsfazfdul
```

Şekil 1. Test sonucu

2. ÇIKTILAR

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

3. SONUÇ

Kripto işlemlerinde oluşturulan rastgeleliğin kırılmaması için kullanılabilecek bir yapı oluşturulmuştur.

Referanslar

[1] 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.