

RRE Şifreleme Algoritması

Nasıl Şifreler?

Girilen metnin harf sayısına göre anahtar dizisinin uzunluğu belirlenir, anahtarın içine belirlenmiş dizinin uzunluğu kadar rastgele 1 ile 5 arası sayılar tanımlanır ve bu sayılara göre şifrelenecek metnin harflerinin aralarına yine rastgele şekilde harfler yerleştirilir. Şifrelenmiş bu metni çözmek için mutlaka “Anahtar” dizisi elimizde bulunmalıdır.

Şifrelenmesini istediğiniz metni, sisteme her girdiğinizde farklı şifrelenmiş metin ve anahtar üretecektir ama bu şifrelenmiş metinleri ve anahtarları kullanarak, şifrelenmiş metinleri deşifre ettiğinizde her seferinde aynı sonuçla karşılaşacaksınız. Mesela şifrelenmesini istediğiniz metin “bilgisayar” olsun bu kelimeyi 10 kere sistemde şifreleyin hepsinde farklı anahtar ve şifrelenmiş metin üretecektir ama bu 10 şifrelenmiş metni anahtarlarıyla deşifre ederseniz, 10’unda da şifreleyerek gizlenmiş olan metne yani “bilgisayar” kelimesine ulaşırsınız. **Programımız aynı metni birden fazla tamamen farklı şekilde şifreleyebilir ve her deşifre işleminde doğru sonucu size verir.**

Bu program karakter ayırt etmeksizin aklınıza gelebilecek her türlü dilden harfi şifreleyebilir. Harften dolayı bir hata vermez.

Program Nasıl Çalışır?

```
---RRE ALGORİTMASI---
RRE : Random Reversible Encryption (Rastgele Geri Dönüşümlü Şifreleme)

Lütfen isminizi yazınız: Ramazan
UYARI!: Şifrelenecek Metni Lütfen Büyük Harflerle Girmeyiniz. Çünkü Kırılması Kolaylaşacaktır.
Merhaba Ramazan, lütfen şifrelenecek metni gir: |
```

Python ile **RRE şifreleme Algoritmasını** çalıştırınız. RRE’nin açılımını ve Türkçe karşılığını size sunacaktır. Hemen altına isminizi girmeniz için bir seçenek sunar. İsmınızı yazıp devam ettiğinizde size bir uyarıda bulunur. Şifrelenecek metni büyük harflerle yazarsak; kendi metnimizin harfleri, şifrelenmiş metnin içerisinde büyük harflerle kendini belli eder ve anahtara ihtiyaç duymadan kolayca çözülebilir bu yüzden küçük harflerle girmeye özen göstermeliyiz. Lakin ben programın nasıl çalıştığını size daha kolay ve anlaşılır gösterebilmek için büyük harflerle bir metin yazacağım. Kullanacağınızda kesinlikle küçük harfleri kullanın birazdan nedenini daha iyi anlayacaksınız.

```
Run: RRE Şifreleme Algoritması x
C:\Anaconda3\python.exe "C:/Users/rmzns/Desktop/Program Projeleri/PyCharm/RRE Şifreleme Algoritması.py"

---RRE ALGORİTMASI---
RRE : Random Reversible Encryption (Rastgele Geri Dönüşümlü Şifreleme)

Lütfen isminizi yazınız: Ramazan
UYARI!: Şifrelenecek Metni Lütfen Büyük Harflerle Girmeyiniz. Çünkü Kırılması Kolaylaşacaktır.
Merhaba Ramazan, lütfen şifrelenecek metni gir: MERHABA

-----
Şifrelemek İstediğin Metin: MERHABA
Girdiğin Metnin Şifrelenmiş Hali: MşğmpEtuRakHojAkzhzeBzAdigd
Şifrelenmiş Metni Çözmek İçin Anahtar: [4, 2, 2, 2, 5, 1, 4]
Şifrelenmiş Metnin Anahtar İle Çözölmüş Hâli: MERHABA
-----

Ramazan, şifrelenmiş olan metninizi çözöüp kullanabilmek için lütfen verilen şifrelenmiş metni ve anahtarı saklayınız.
Şifrelenmiş Metin: MşğmpEtuRakHojAkzhzeBzAdigd
Anahtar: [4, 2, 2, 2, 5, 1, 4]
-----

Şifreleme İşlemi Başarıyla Tamamlandı
Görüşmek Üzere Ramazan...

Process finished with exit code 0
```

Şifrelemek istediğimiz metni girdim ve anlatımın daha anlaşılır olması için büyük harflerle girdim.

Metnimiz “MERHABA” yı yazınca enter dediğimiz anda program bize metnin şifrelenmiş halini, deşifre edebilmek için anahtar ve metnin çözölmüş halini bize sunar. Sonrasında ürettiğimiz şifrelenmiş metinleri deşifre edebilmemiz için elde ettiğimiz şifrelenmiş metni ve anahtarı saklamamızı ister. İşlemin tamamlandığını hakkında bize bilgi verir ve program bize girdiğimiz isimle hitap ederek son vedasını eder.

```
-----
Şifrelemek İstediğin Metin: MERHABA
Girdiğin Metnin Şifrelenmiş Hali: MşğmpEtuRakHojAkzhzeBzAdigd
Şifrelenmiş Metni Çözmek İçin Anahtar: [4, 2, 2, 2, 5, 1, 4]
Şifrelenmiş Metnin Anahtar İle Çözölmüş Hâli: MERHABA
-----
```

Girdiğimiz metni daha kolay görebilmek için büyük harflerle girmiştik.

Şimdi anahtar ve şifrelenmiş metin arasındaki ilişkiyi kullanarak programımız şifrelenmiş metni nasıl deşifre ediyor onu anlatacağım.

Anahtar dizimiz şu şekilde [4,2,2,2,5,1,4] bu demek oluyor ki M harfinin önüne 4, E harfinin önüne 2, R harfinin önüne 2, H harfinin önüne 2, 2. A harfinin önüne 5, B harfinin önüne 1, 3. A harfinin önüne ise 4 tane rastgele şekilde harf yerleştir anlamına geliyor. Bu anahtar da rastgele oluşturulan harfler gibi her defasında aynı şifrelenecek metin kullanılsa bile rastgele şekilde 1 ve 5 sayıları arasından üretilir. **Yani programımız aynı metni birden fazla tamamen farklı şekilde şifreleyebilir ve her deşifre işleminde doğru sonucu size verir.**

Yukarıdaki resimde de göröldüğü gibi “MERHABA” yı her harfinin önüne **anahtarda belirtilen sayılara göre rastgele şekilde harflerle** şifreliyor. Ben daha kolay gözükmesi için metni büyük harflerle yazdım.

Küçük harflerle yazsaydık:

Girdiğimiz metnin şifrelenmiş hali şu şekilde olurdu: “mşğmpeturakhojakzhzebzadigd” ve bunu asla anahtar olmadan çözemeyiz.

Anahtara göre ayırırsak: "m4e2r2h2a5b1a4" buradaki her bir sayı üretilmiş random harfleri temsil ediyor. Üretilmiş random harfleri Şifrelenmiş metinden anahtar yardımıyla silerseniz sonuç: "merhaba" yı yani şifreleyerek gizlediğimiz metni elde etmiş olurduk.

NOT: Programı tekrar çalıştırıp aynı şekilde şifrelenecek metne tekrar merhaba yazarsak bize aynı şifre ve anahtarı sunmaz ama deşifre edildiğinde aynı metni bize verir.

Örnek:

1. Deneme:

2. deneme:

Şifrelemek İsteddiğiniz Metin: merhaba	Şifrelemek İsteddiğiniz Metin: merhaba
Girdiğiniz Metnin Şifrelenmiş Hali: mdezşiyrotşmhpogcajssbjbgföar	Girdiğiniz Metnin Şifrelenmiş Hali: mgöçejrirkjhjavbşfihagbnf
Şifrelenmiş Metni Çözmek İçin Anahtar: [1, 4, 4, 4, 5, 3, 1]	Şifrelenmiş Metni Çözmek İçin Anahtar: [3, 1, 4, 1, 1, 4, 4]
Şifrelenmiş Metnin Anahtar İle Çözölmüş Hâli: merhaba	Şifrelenmiş Metnin Anahtar İle Çözölmüş Hâli: merhaba

Sonuç: 2 denemede de göröldüğü gibi 2'sinde de farklı şifrelenmiş bir metin ve anahtar üretildi ama ikisi de anahtarlarıyla deşifre edildiğinde aynı şifrelenmek istenen metne ulaşırız yani "merhaba"ya.

Programın Algoritması ve Açıklamaları:

Açıklamalar "#" ile başlayan cümlelerdir.

```
import random # Random modöölünü kullanacağımız için sisteme import ediyoruz.

print(" ")
print("---RRE ALGORİTMASI---")
print("RRE : Random Reversible Encryption (Rastgele Geri Dönüşümlü Şifreleme)") print("
")
# Yukarıdaki kısım programımızın giriş ve kendini tanııtma kısmıydı.

isim = input("Lütfen isminizi yazınız: ") # Burası programımızın kullanıcıya hitap etmesi için isim aldığı yer. print("UYARI!:
Şifrelenecek Metni Lütfen Büyük Harflerle Girmeyiniz. Çünkü Kırılması Kolaylaşacaktır.") # Büyük harf uyarısı.

sifrelenecek_metin = input("Merhaba"+" "+ isim + ", "+"+"lütfen şifrelenecek metni gir: ") # Yukarıdaki satırda ismimizle hitap
ederek şifrelenecek metin isteniyor ve böylece "sifrelenecek_metin" değışkenini tanımlıyoruz.

alfabe = ["a","b","c","ç","d","e","f","g","ğ","h","i","ı","j","k","l","m","n","o","ö","p","r","s","ş","t","ü","ü","v","y","z"]
sifrelenmiş_metin = "" anahtar = [] # Alfabe, Şifrelenmiş Metin, Anahtar dizisi ve Çözölmüş Metni de sisteme
tanımlıyoruz.
cozulmus_metin = ""
```

```
for i in sifrelenecek_metin: sifrelenmis_metin += i rastgele_sayı = random.randint(1,5) #  
Rastgele olarak 1 ile 5 arasında rakamlar üretmeye yarar.  
    anahtar.append(rastgele_sayı) # Üretilen sayıları append diyerek anahtar dizisinin içerisine yazar.  
  
    for x in range(rastgele_sayı): harf = random.choice(alfabe) # Girdiğimiz metnin arasındaki  
random harfler burada üretiliyor.  
        sifrelenmis_metin += harf  
  
for i in range(len(anahtar)): # Anahtardaki random sayılarının uzunluğunu alır. index = 0  
# Şifrelenmiş metindeki karakterleri çözerken 0.indexten başlanmasını sağlar.  
  
    for x in anahtar:  
        if len(cozulmus_metin) <= len(anahtar)-1: # Eğer çözülmüş metnin uzunluğu anahtarın uzunluğundan 1  
eksikse cozulmus_metin += sifrelenmis_metin[index] # Çözülmüş metin = çözülmüşmetin+şifrelenmiş  
metin(index) else: # Değilse break  
                # index = index+x+1 şeklinde yap.  
  
        index += x + 1  
  
print("-----") print("Şifrelemek  
İstediğin Metin: ",sifrelenecek_metin) print("Girdiğin Metnin Şifrelenmiş Hali: ",sifrelenmis_metin) # Bu alan elde etmek  
istediğimiz verileri ekrana yazdırma kısmı. print("Şifrelenmiş Metni Çözmek İçin Anahtar:",anahtar)  
print("Şifrelenmiş Metnin Anahtar İle Çözülmüş Hâli: ",cozulmus_metin)  
print("-----") print(isim + ", "+"  
"+"şifrelenmiş olan metninizi çözüp kullanabilmek için lütfen verilen şifrelenmiş metni ve anahtarı saklayınız.") print("Şifrelenmiş  
Metin: ",sifrelenmis_metin) print("Anahtar: ",anahtar) # Bu alan ise ismimizle hitap ederek bize şifrelenmiş metnin ve anahtarın  
saklanması uyarısını yapıyor. print("-----"  
---) print("Şifreleme İşlemi Başarıyla Tamamlandı") # Bu alan son alanımız. Kullanıcıya işlemin tamamlandığının bilgisini veriyor  
print("Görüşmek Üzere"+" "+isim+"...") # Ve ismimizle hitap ederek kullanıcıya vedasını ediyor.
```