AMAÇ : Bu uygulamanın amacı kişiye kriptoloji alanındaki bilgilerini test etmek için ortam sağlamaktır.

ÖNBİLGİ :

Base 64 decoder:

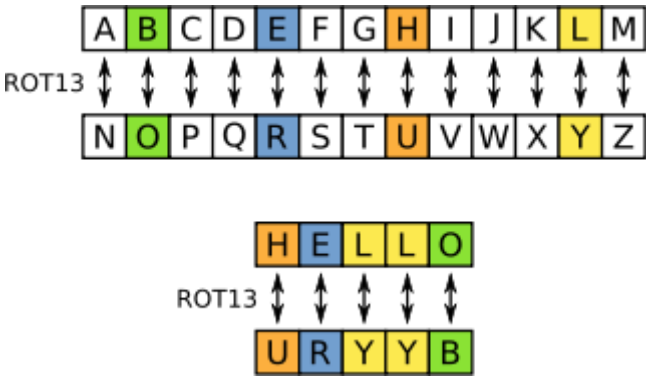
Base64 ikili verilerin (binary data) sadece ASCII karakterlerini kullanan ortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şemasıdır. Bir base64 kodlamasının uzunluğu daimi olarak 4' ün katları şeklindedir, uzunluğu 4' ün katı olmayan hiçbir metin geçerli bir base64 metin değildir. base64 kodlaması bitmiş bir verinin uzunluğu 4'ün katı değilse, gerektiği kadar '=' karakteri çıktının sonuna eklenir, örneğin uzunluğu 10 olan bir çıktının sonuna '==' eklenmelidir. Base64 kodlaması en sık MIME (Multipurpose Internet Mail Extensions) standardı uygulamalarında yani elektronik postaya ikili dosya (binary file) eklenmesi işleminde kullanılır. Kodlanmış dosya orijinal haline göre ortalama 33% oranında büyür.[1] Base 64 bir şifreleme algoritması değildir. Binary verilerin, ASCII kullanılan ortamlarda iletimi ve saklanmasına olanak sağlayan bir kodlama şemasıdır.

Örnek:

Base64:VmlraXBlZGk=
Örnekteki her bir karakter bir bayt büyüklüğündedir.

ROT 13 Şifreleme :

ROT13 (Rotate13) yer değiştirme yöntemi kullanan bir Caesar(Sezar) şifreleme türüdür. Mantık olarak ingiliz alfabesindeki bir harfin 13 harf sonraki harf ile eşleşmesidir. Harflerin eşleşme tablosunu Şekil 1'de görüldüğü gibidir. Şekilde görüldüğü gibi "HELLO" metini ROT13 şifreleme algoritması ile "URYYB" şifreli metnine dönüşmektedir.



Şekil 1 ROT13 Eşleştirme Tablosu

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

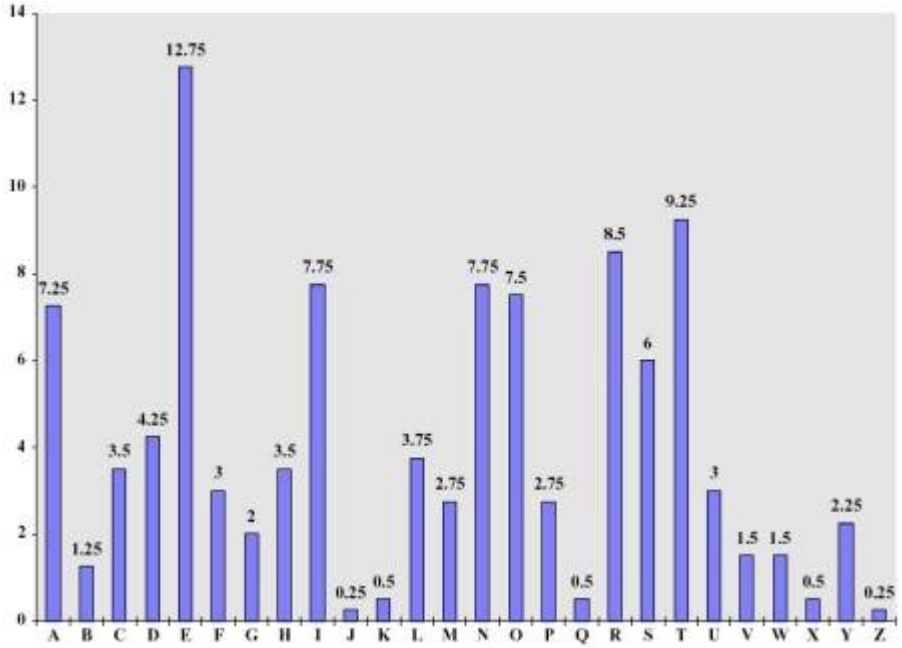
a) Cryptool (https://www.cryptool.org/en/jcryptool) uygulamasını indirip bilgisayarınıza kurun.

b) Putty (http://www.putty.org/) veya SSH bağlantısı için kullanılabilecek farklı bir SHH bağlantı aracını indirerek SHH bağlantısı yapabilecek ortamı sağlayın.

c) Base 64 decoder konusu bilgi sahibi olunması beklenmektedir.

d) ROT 13 decoder hakkında bilgi sahibi olunması beklenmektedir.

e) İngiliz diline ait frekans analiz tablosunu inceleyin.



Şekil 2 İngilizce Harf Freakans Tablosu [3]

f) The black chammber adresini ziyaret edin ve İngiliz alfabesinde yer alan unigram, bigram ve threegram en sık eşleşmeleri bulun.

İngiliz Alfabesinde;

Order Of Frequency Of Single Letters
E T A O I N S H R D L U

Order Of Frequency Of Digraphs
th er on an re he in ed nd ha at en es of or nt ea ti to it st io le is ou ar as de rt ve

Order Of Frequency Of Trigraphs
the and tha ent ion tio for nde has nce edt tis oft sth men

Order Of Frequency Of Most Common Doubles
ss ee tt ff ll mm oo

Order Of Frequency Of Initial Letters
T O A W B C D S F M R H I Y E G L N P U J K

Order Of Frequency Of Final Letters
E S T D N R Y F L O G H A K M P U W

One-Letter Words
a, I

Most Frequent Two-Letter Words
of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am

Most Frequent Three-Letter Words
the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use

Most Frequent Four-Letter Words
that, with, have, this, will, your, from, they, know, want, been, good, much, some, time

g) **Vigenere Şifreleme :**

Vigenere tablosu, kriptografide Vigenere şifrelemesi için kullanılan ve Fransız şifrecisi Blaise de Vigenere'e atfedilen bir tablodur. Bu tablo şifre için gerekli her harfin hangi harf ile değiştireleceğini gösterir. Harflerin değiştirilmesi için birçok alfabe kullanılır. Her harfin kelimedeki sırasına göre şifreleme alfabesi de değişir. Böylece aynı harflerin aynı harfler ile değiştirilmesi engellenmiş olur. Çoklu alfabe kullanma yöntemiyle şifrenin frekans analizi ile çözülmesi zorlaştırılmış olur. Vigenere şifrelemesi Sezar şifrelemesinin geliştirlmiş halidir. Sezar şifrelemesi için harflerin değiştirilmesi için bir tek alfabe kullanılırken Vigenere şifrelemesinde birden fazla alfabe kullanılır. Şifreleme için bir anahtar seçilir ve bu anahtara göre her harf kelime içindeki sırasına göre değişik bir alfabeyle şifrelenir. Anahtarla bu şifreleme Sezar şifrelemesine göre aynı kolaylıkla yine deşifre edilebilinir. [4]

B. Uygulamanın Yapılışı:

a) The Krypton war game (http://overthewire.org/wargames/krypton/) sayfasını ziyaret edin.

b)

Level 0 :

```
S1JZUFRPTklTR1JFQVQ=
```

Yukarıdaki kodun neden base64 kodu olduğunu açıklayın. Herhangi bir base64 decoder yada cryptool kullanarak bu kodu decode edin.

```
#!/usr/bin/python
# Simple base 64 decoder
import base64

keyin = "S1JZUFRPTklTR1JFQVQ="
keyout = base64.b64decode(keyin)

print(keyout)
```

Level 1 :

Level 0'da elde edilen şifreyi kullanarak. krypton.labs.overthewire.org adresini SSH ile bağlanın.

Krypton1 klasörüne girin ve README dosyasını okuyun. krypton2 dosyası içiresinde yer alan şifreli metnin şifrelenme algoritmasını söyleyin ve daha önce yazdığınız sezar deşifreleyiciyi kullanarak metni decrypt edin.

```
"YRIRY GJB CNFFJBEQ EBGGRA".decode(encoding="ROT13")
 u'LEVEL TWO PASSWORD ******'
```

Level 2 :

Elde ettiğiniz şifreyi kullanarak krypton2 kullanıcı adı ile sunucuya bağlanarak krypton2 klasörüne girin ve README dosyasında talimatları okuyun.

Krypton3 dosyasının şifreleme yöntemi/algoritması nedir?

Kriptanaliz yöntemlerini yada brute-force atak yöntemi kullanarak metni decrypt edin.

Brute-force atak yöntemi için en fazla kaç deneme yapılacağını söyleyin?

İpucu : Şifreleme algoritmasını kullanarak alfabeyi şifreleyip, shift miktarnı öğrenebilirsiniz

Level 3 :

Elde ettiğiniz şifreyi kullanarak krypton3 kullanıcı adı ile sunucuya bağlanarak krypton3 klasörüne girin ve README dosyasındaki talimatları okuyun.

Şifreleme yöntemini açıklayın. Verilen ipuçlarını okuyup bunların yapılacak deşifreleme işlemi için ne tür bir yönlendirme sağladığı üzerine tartışın.

İpucu : http://www.richkni.co.uk/php/crypta/freq.php adresinde bulunan frekans analiz uygulamasını kullanarak ngram analiz yapabilirsiniz.

Level 4 :

Elde ettiğiniz şifreyi kullanarak krypton4 kullanıcı adı ile sunucuya bağlanarak krypton4 klasörüne girin ve README dosyasındaki talimatları okuyun.

Kullanılan şifreleme yöntemini açıklayın.

http://smurfoncrack.com/pygenere/pygenere.php adresindeki vigere kod çözücüyü yada farklı vigere decrypter kullanarak kullanarak. Krypton5 dosyasında bulunan şifreli metni çözün.

Çözümler :

Level 0:

Level 1: ROTTEN

Level 2: CAESARISEASY

Level 3: BRUTE

Level 4 : FREKEYFRE

Level 5:

ANALİZ :

- Özet fonksiyonlar arasındaki farkları ve güvenlik değerini tartışın.
- Veri şifreleme için özet fonksiyonların güvenlik seviyesini tartışın.
- Aynı özet değere sahip iki farklı doküman olabilir mi ?

REFERANSLAR :

1- Base64 encoding, https://tr.wikipedia.org/wiki/Base64, son erişim tarihi : 09/12/2015

2- ROT13 şifreleme, http://www.sctzine.com/rot13-converter-rot13-sifreleme-yontemi/, son erişim tarihi : 09/12/2015

3- İngilizce harf frekans tablosu, http://sjsu.rudyrucker.com/~haile.eyob/paper/, son erişim tarihi : 09/12/2015

4- Vigenere Şifreleme, https://tr.wikipedia.org/wiki/Vigenere_tablosu, son erişim tarihi : 09/12/2015