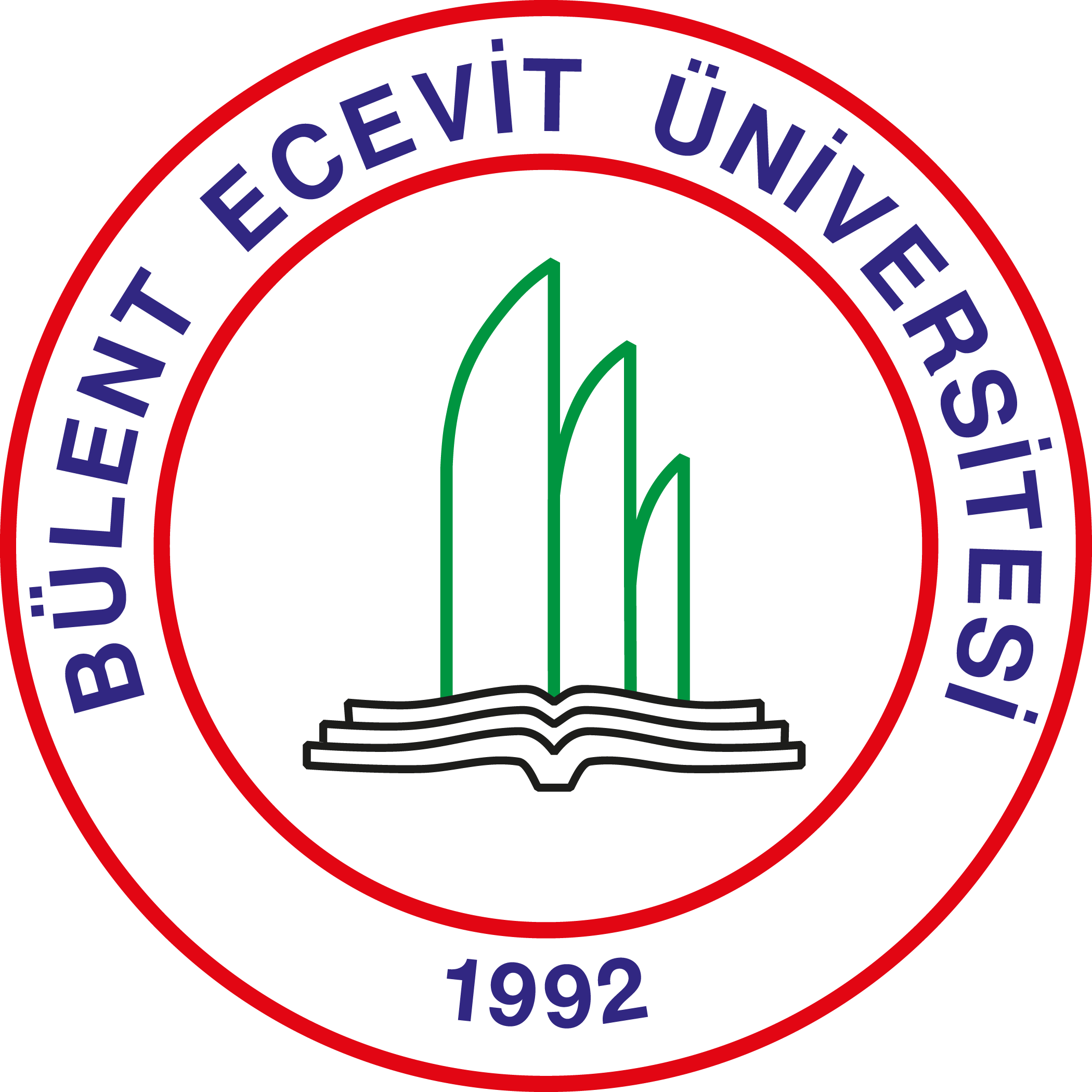
**PROJE RAPORU**

**ŞİFRE KIRICI(PASSWORD CRACKER)**



**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ (İ.Ö.)**

**SALİH ÖZTÜRK**

**170106206023**

**HAZİRAN 2020**

**PROJE ADI:** Decoder

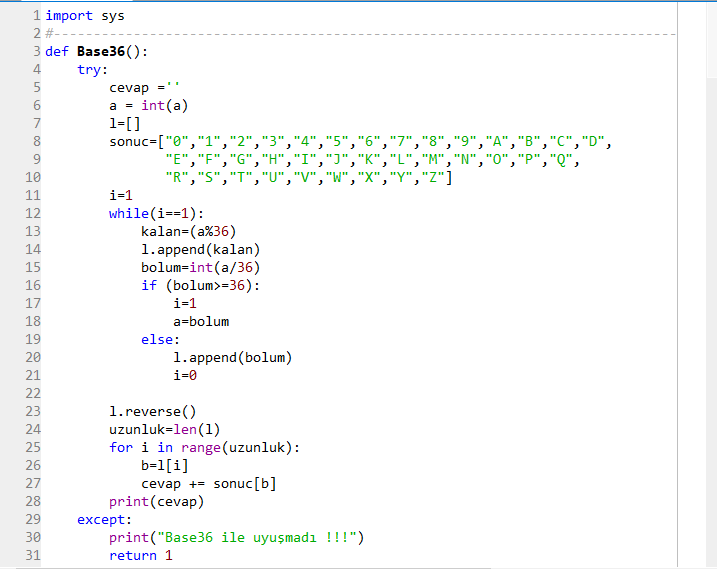
**PROJENİN TÜRÜ:** Kriptoloji

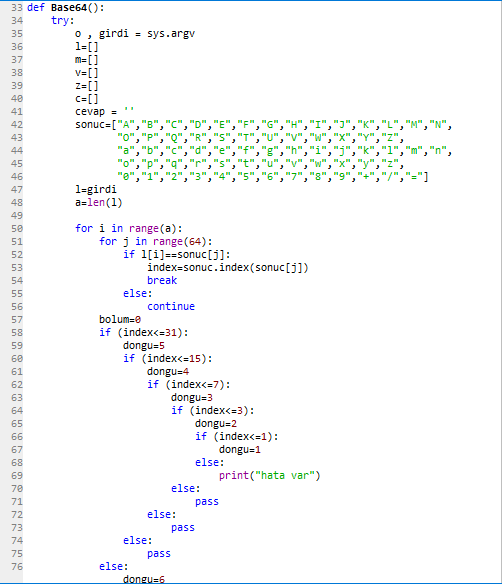
**PROJE AMACI**: Bu proje kriptoloji alanında kullanılan algoritmaların şifrelerini çözmek ve zafiyet arayan siber güvenlik çalışanlarına yardımcı olmak ayrıca CTF yarışmacıları gibi siber güvenlikle uğraşan kişileri karşılarına çıkan şifreleme türlerindeki şifreli metinleri site site dolaşıp her şifreleme türü için farklı site bulma uğraşından ve bu sayede de zaman ve enerji kaybından kurtarma amacıyla yapmış olduğumuz bir programdır. Bu proje bitiminde TÜBİTAK ‘ a ve ayrıca CTF yarışmacıları için ücretli bir yazılım olarak piyasaya sunulması planlanmaktadır.İçerisinde CTF yarışmalarında yoğunlukla kullanılan şifreleme türleri yer almaktadır.

**MATERYAL VE YÖNTEM :**Python programlama dili kullanılarak yapılan bu program,genel olarak kullanılan şifreleme algoritmalarının matematiksel hesaplaması yapılarak şifreyi çözümü her algoritma için ayrı ayrı fonksiyon halinde yazılmıştır**.**

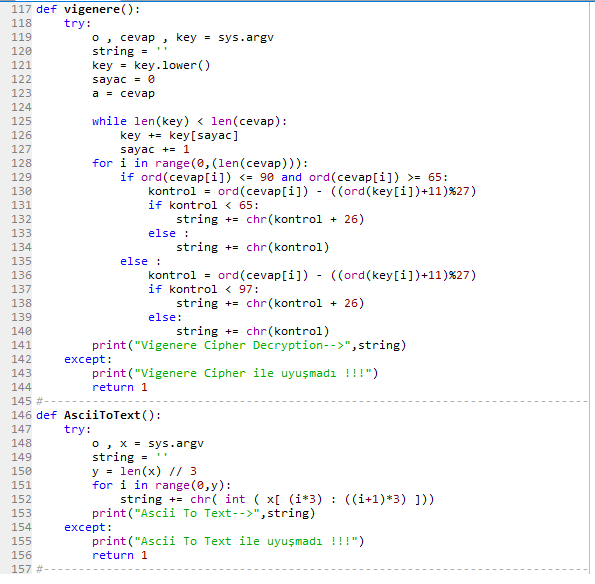
**PROGRAMIN ÇALIŞMA PRENSİBİ**

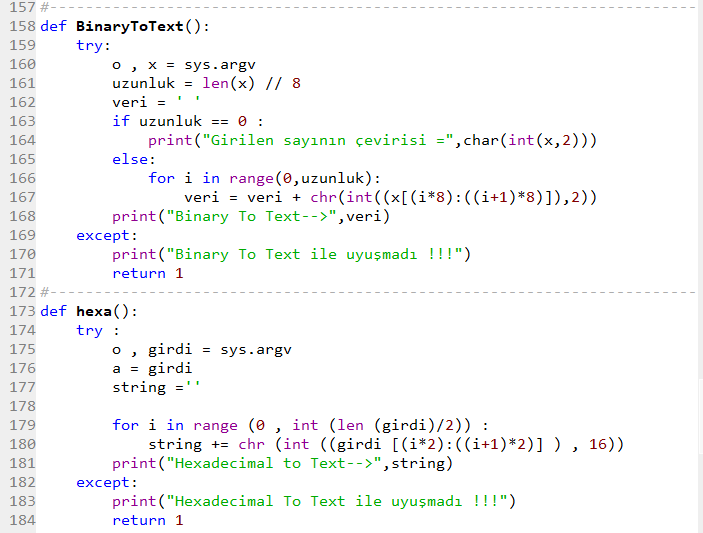
Bu programda dışarıdan şifreli metin ve gerekli durumlarda şifreli metnin anahtarı alınacaktır. Ayrıca bazı ayırt edilmesi zor şifreleme türlerinde programın hangi şifreleme türüne göre girdiyi çözeceği de argüman olarak eklenecektir.Program çalıştıktan sonra ise şifresi kırılmış metin ekrana bastırılacaktır.

**BASE36 ŞİFRELEME ALGORİTMASI**

**BASE64 ŞİFRELEME ALGORİTMASI ÇÖZÜMÜ**

**BASE64 DEVAMI**

**VİGENERE ve ASCII TO TEXT ALGORİTMALARI ŞİFRE ÇÖZÜMÜ**

**BİNARY TO TEXT ve HEXADECİMAL TO TEXT ŞİFRE ÇÖZÜMÜ**

**XOR TO TEXT ve CAESAR ALGORİTMALARI ŞİFRE ÇÖZÜMÜ**

**SONUÇ:**

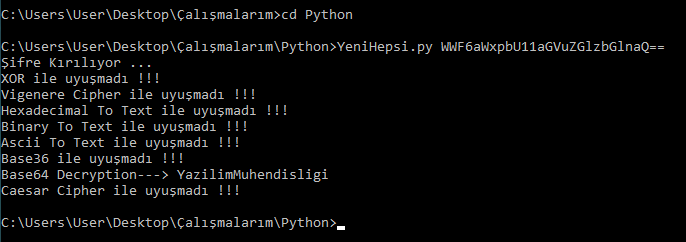
**PROGRAM ÇALIŞTIRILDIĞINDA ELDE EDİLEN PROGRAM ÇIKTILARI**

“YazilimMuhendisligi” kelimesi şifreli olarak terminale yazıldığında çıktı olarak şifreli mesajı decode ediyor ve gerçek sonuç ekrana yazdırılıyor.

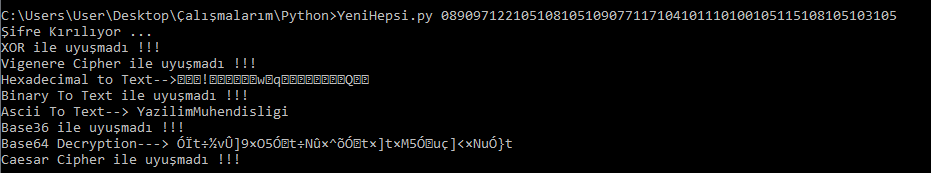
: Şifreli metin

: Anahtar (Bazı şifrelerin çözülmesi için gerekli kelime veya sayı)

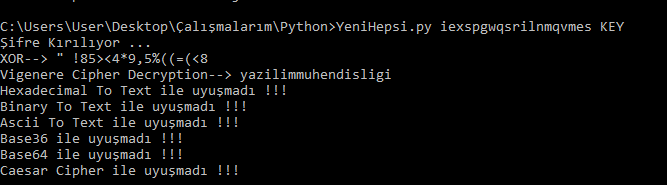
: Şifresi çözülmüş metin

**Base64**

Base64, PHP programlama dili içerisinde 8 bitlik verileri 64 bite çevirmek amacıyla kullanılan bir kodlama tekniğidir. 8 bit değerine sahip olan veriler ile 64 bitlik veriler arasında farklı katmanlı iletişimlerin meydana gelmemesi için bu basit kodlama tekniği kullanılır. Böylece iletişim sırasında katmanlardan dolayı meydana çıkabilecek veri kaybı önlenir.

**Ascii to text**

Bu şifreleme türünde girilen şifreli metin, karakterlerin ascii karşılıklarına gelen sayılardan oluşmaktadır. Decoderde ise girilen sayının asci tablosundaki karşılığı olan karakter bulunarak şifreli metin çözülür.

**Vigenere**

İlkel Şifreleme yöntemlerinden birisidir. Kaydırma Şifrelemesi ve Yerine koyma şifrelemesi gibi şifrelemelerden en önemli farkı şifrenin her harfe aynı şekilde değil bir harf bloguna uygulanmasıdır. Örnek olarak “mesaj” kelimesini “ali” şifresi ile şifrelemek isteyelim bu durumda:

mesaj -> 13 5 19 1 10, ali -> 1 12 9

şifreleme işlemi için şifre ile harfler sırasıyla toplanır:

13 05 19 01 10

01 12 09 01 12

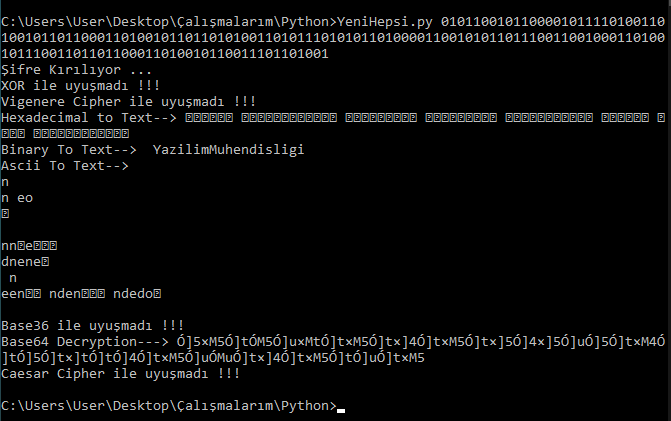
—————

14 17 28 02 22

14 17 02 02 22

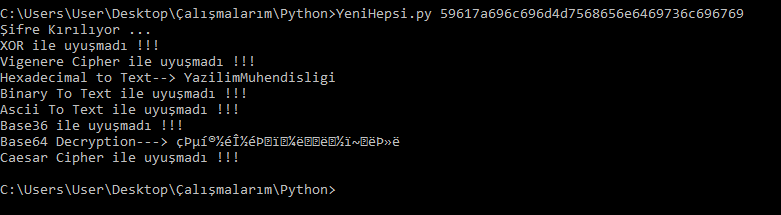
dolayısıyla şifreli metin “nqbbw” olarak bulunur. Açan taraf şifrelemenin tersini yani sırasıyla harflerden anahtarı çıkararak metni bulabilir.

**Binary to text**

****

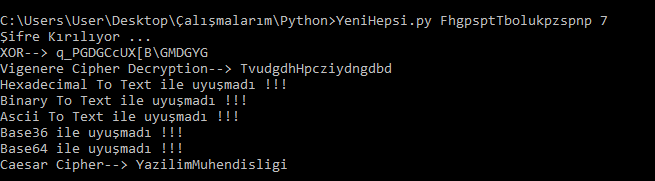
Binary to text decoderda ikili tabanda bulunan 1 baytlık sayı grubu alınır. Bu alınan sayı odalık tabana dönüştürülür. Bu dönüşen ondalık tabanda bulunan sayının ascii tablosunda karşılık geldiği karakter alınır. Bu bütün şifreleme böbütün şifreleme boyunca devam eder ve bütün karakterler birleştirilerek şifrenin kırılmış hali bulunmuş olur.

**Hexadecimal to text**

****

Girilen 16’lık tabandaki sayıları decimal (10’luk) sayı sistemine çevirip bu decimal sayı sistemindende ascii karşılıklarından şifreyi bulan decoderdir.

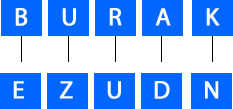
**Caesar cipher**

****

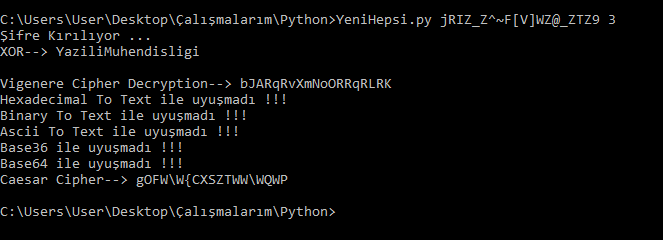
Sezar savaş döneminde önemli bilgileri bu şifreleme tekniği ile yollarmış.

Bu şifreleme tekniği şöyle istemekte. Sizin şifrelenmesini istediğiniz bir kelime ya da veri mevcut diyelim. Bizim bir anahtar değer belirlememiz gerekmekte. Bu anahtar değeri bir rakam olmalı. Bu anahtar değeri kadar verilen kelimedeki harfleri öteliyoruz.

BURAK kelimesini şifreleyelim. Anahtar değeri 3 olsun. O halde her harfi 3 harf sonrasına gelen değer şeklinde yazacağız ve şifrelenmiş olacak. Kısaca şöyle;



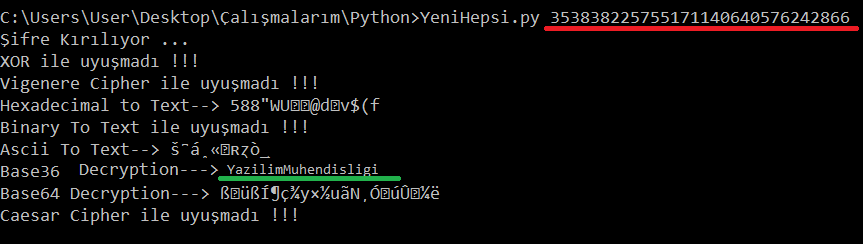
**Xor**

****

Veri güvenliğinde kullanılan en basit şifreleme algoritmalarından birisidir. Şifreleme ailesi olarak blok şifreleme (Block Cipher) ailesinden simetrik şifreleme olarak kabul edilebilecek olan bu şifreleme algoritmasında mesaj önce verilen blok boyutunda parçalara bölünür. Ardından her parça anahtar ile Yahut (XOR) işlemine tabi tutulur. Çıkan sonuçlar birleştirilerek şifreli mesaj elde edilir.

Alıcı taraf mesajı açmak için yine blok boyutu kadar parçalara böler ve anahtar ile ikinci kere Yahut(XOR) işlemine tabi tutar. Sonuçta çıkan mesaj orjinal mesajdır.

**Base36**

****

Taban 36 şifre aritmetik baz değişimi (dönüşüm prensibini kullanır tabanı 36 tabanına 10) içerir. Böylece, kelimeler temel 36'da (36 alfasayısal sembol olarak ABCDEFGHIJKLMNOPQRSTUVWXYZ ve 10 rakam 0123456789 alfabesinin 26 harfiyle) yazılır ve daha sonra temel 10'da bir sayıya dönüştürülür.