1. **ACTIVIDADES**

**Cifrado de Vignere**

1. Implementar un cifrador de Vignere, donde se pueda seleccionar el módulo, alfabeto módulo 27 o módulo 191 (ASCII), ingresar el texto claro (en archivo o por interface) y genere la cifra resultante

**Ejercicio 1:**

def vignere\_cifrado(archivo,clave):

f = open(archivo,encoding="utf8")

g = open("cifrado.txt","w")

j=0

c=""

abc="ABCDEFGHIJKLMNÑOPQRSTUVWXYZ"

alfabeto\_size=len(abc)

for linea in f:

for i in linea:

m=abc.find(i)

k=abc.find(clave[j])

ci=(m+k)%alfabeto\_size

g.write(abc[ci])

if(j<len(clave)-1):

j+=1

else:

j=0

g.close()

f.close()

**LLAMADA**

vignere\_cifrado("texto\_plano.txt","CIELO")

**SALIDA**

JMVWDUW

def vignere\_descifrado(archivo,clave):

f = open(archivo,encoding="utf8")

g = open("descifrado.txt","w")

j=0

c=""

abc="ABCDEFGHIJKLMNÑOPQRSTUVWXYZ"

alfabeto\_size=len(abc)

for linea in f:

for i in linea:

c=abc.find(i)

k=abc.find(clave[j])

mi=(c+(alfabeto\_size-k))%alfabeto\_size

g.write(abc[mi])

if(j<len(clave)-1):

j+=1

else:

j=0

g.close()

f.close()

**LLAMADA**

vignere\_descifrado("cifrado.txt","CIELO")

**SALIDA**

HERMOSO

1. Verificar cifrando “Dentro de veinte años estarás más decepcionado por las cosas que no hiciste, que por las que hiciste. Así que suelta las amarras. Navega lejos del puerto seguro. Atrapa los vientos alisios en tus velas. Explora. Sueña. Descubre.” Usando la clave SABIDURIA

**EJERCICIO 2:**

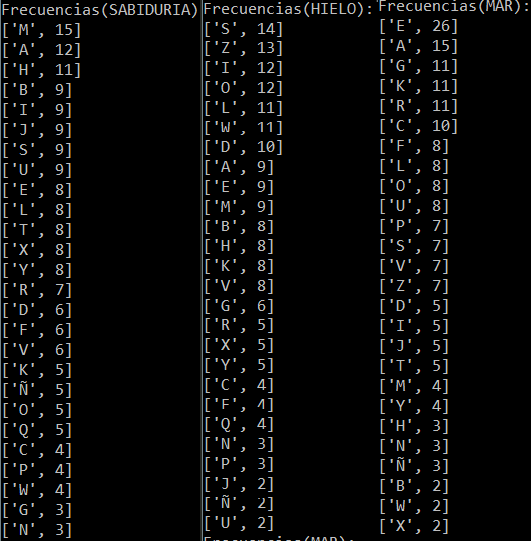
**CIFRADO:**

VEÑBUJUMVWIÑBHUFWSWSUIUUKTALDFKHKTPOFAEWSJJSALCPADNICEFOIPFCKBEJUFXRMCISJUFOLWZATWATPTOVAUWLUIÑUKIMSRSIVHRDEYAMMMJKLEDPVMUÑGAEYUSWDÑJIPSLPAYCVUTHSBSLNZWSWNUCVPVSALEYXÑJJISNEOIGYKKUTRF

**DESCIFRADO:**

DENTRODEVEINTEAÑOSESTARASMASDECEPCIONADOPORLASCOSASQUENOHICISTEQUEPORLASQUEHICISTEASIQUESUELTALASAMARRASNAVEGALEJOSDELPUERTOSEGUROATRAPALOSVIENTOSALISIOSENTUSVELASEXPLORASUEÑADESCUBRE

1. Verifica el resultado obtenido a partir del cifrador **Criptoclásicos v2.1 (**[http: //www.criptored.upm.es/software/sw\_m001c.htm](http://www.criptored.upm.es/software/sw_m001c.htm) ) haciendo las capturas de pantalla respectivas para los módulos 27 y 191
2. Muestre las frecuencias de cada letra del mensaje original usando como claves SABIDURIA, HIELO y MAR, compare y concluya sobre la variación de las frecuencias en base a la longitud de la clave

****

* Al variar el tamaño de la clave, los resultados de frecuencias cambian aumentando el número de frecuencias de una letra en específico, lo cual puede facilitar para determinar que caracteres fueron usados para la clave.

1. Desarrolle un algoritmo que encuentre el texto claro si recibió la cifra AEYZRNTZDJSEVSJSFAÑSXRFVHKOFTZDJLPZLUO, y se sabe que ha cifrado con la clave PEDRONAVAJA

**EJERCICIO 5:**

def vignere\_descifrado\_5(archivo,clave):

f = open(archivo)

g = open("texto\_desencriptado.txt","w")

j=0

ii=0

c=""

alfabeto\_size=len(abc)

#print("linea:",len(linea))

clave = duplicar\_clave(archivo,clave)

print (clave)

for linea in f:

for i in linea:

c=abc.find(i)

k=abc.find(clave[j])

mi=(c+(alfabeto\_size-k))%alfabeto\_size

print(abc[mi])

g.write(abc[mi])

if(j<len(clave)-1):

j+=1

else:

j=0

g.close()

f.close()

def duplicar\_clave(archivo,clave):

f = open(archivo)

ii=0

for linea in f:

for i in linea:

print("clave:",len(clave))

if(len(clave)<len(linea)):

clave=clave+clave[ii]

ii+=1

else:

break

return clave

**LLAMADA:**

vignere\_descifrado\_5("texto\_encriptado.txt","PEDRONAVAJA")

**SALIDA:**

LAVIDATEDASORPRESAEZKXCBSPVCFYZUJVMWTGC

1. Usando el software anterior, verifique el resultado, eligiendo el cifrado Vignere con módulo 27
2. Usando matemáticas discretas, descifre manualmente YGVMSSKKOX si la clave fue FORTALEZA en un alfabeto de 27 caracteres

**Cifrado con autoclave**

1. Descifre el texto, usando la clave UNODELOSMASGRANDESCRIPTOGRAFOS:

XHGDQESDMPKÑDEEDKNGJZPFJSUIFZOLFCINFJCESVZTGBFXCIUDAYNUUDIZYWWZBEYNVQWIVUNKZEPHDODQUZZLBDNDRWTHQSERÑIVMLERCMGIFLSORZXTSDIGLOXQSDJHWVCIWQXQJCKMBPOKMPSKMUVIMNJDNBLCSZHXHNYYUIXDBSOXHZLXWVGDJGXHWLTDWKÑSAQIMZLNBVMLXHUOQQXIQGWGUFTWKZKMOKUDNINSIFJDUOZIJBSVVOWFAIEÑGYOWPSOAP

**EJERCICIO 8:**

def vignere\_descifrado\_autoclave(archivo,clave):

f = open(archivo,encoding="utf8")

g = open("textDec.txt","w")

texto=f.read()

cont=0

for i in texto:

x=abc.find(i)

y=abc.find(clave[cont])

z=abc[(x-y)%27]

clave+=z

g.write(z)

cont=cont+1

if(cont==len(clave)):

cont=0

f.close()

g.close()

**LLAMADA:**

vignere\_descifrado("texto\_encriptado.txt","UNODELOSMASGRANDESCRIPTOGRAFOS")

**SALIDA:**

DURANTELAPRIMERAGUERRAMUNDIALWILLIAMFREDERICKFRIEDMANSIRVIOCOMOTENIENTEENLAUNIDADDECRIPTOLOGIADELAFUERZAEXPEDICIONARIAESTADOUNIDENSEDISTINGUIENDOSEPORSUSTRABAJOSYPROEZASENELANALISISDECODIGOSENEMIGOSINVIOLABLESPORLOCUALRECIBIOELRECONOCIMIENTODELGOBIERNOESTADOUNIDENSER

**Ataque de Kasiski**

1. Criptoanalizar el siguiente criptograma mod 27, encontrar la clave y el texto en claro.

MAXYHGAVAPUUGZHEGZQOWOBNIPQKRNÑMEXIGONIICUCAWIGCTEAGMNOLRSZJNLWÑAWWIGLDDZSNIZDNBIXGZLAYMXÑCVEKIETMOEOPBEWPTNIXCXUIHMECXLNOCECYXEQPBWUFANIICÑJIKISCZUAILBGSOANKBFWUAYWNSCHLCWYDZHDZAQVMPTVGFGPVAJWFVPUOYMXCWERVLQCZWECIFVITUZSNCZUAIKBFMÑALIEGLBSZLQUXÑOHWOCGHNYWÑQKDANZUDIFOIMXNPHNUWQOKLMVBNNKRMKONDPDPNMIKAWOXMEEIVEKGBGSFHVADWPGOYMHOIUEEIPGOLENZBSCHAGKQTZDRÑMÑNWTUZIÑCMÑAXKQUWDLVANNIHLÑCQNWGEHIPGZDTZTÑNWÑEEWFUMGIÑXNTWXNVIXCZOAZSOQUVENDNFWUSZYHGLRACPGGUGIYWHOTRMZUGQQDDZIZFWHVVSHCUGOGIFKBXAXPBOBRDVDUCMVTKGIKDRSZLUQSDVPMXVIVEYMFGTEANIMQLHLGPQOHRYWCFEWFOISNÑPUAYINNÑXNÑPGKWGOILQGAFOILQTAHEIIDWMÑEÑXNEPRCVDQTURSK

def Kasiski(archivo):

f = open(archivo)

c=[]

cont=0

ini=0

fin=0

dist=0

for linea in f:

for i in range(0,len(linea),1):

tri=linea[i:3+i]

ini=i+3

for j in range(i,len(linea),1):

auxtri=linea[j:3+j]

if(tri==auxtri):

#j=j+3

dist=(j-ini)

if(dist==-3):

dist=0

c.append([])

for k in range(2):

c[cont].append(None)

c[cont][0]=tri

c[cont][1]=dist

ini=j

cont=cont+1

dist=0

f.close()

lista=[]

for i in range(len(c)):

if(c[i][1]!=0):

lista.append(c[i][1])

print(c[i])

return lista

1. **CONCLUSIONES**

* Este tipo de encriptado tiene mucha facilidad de ser analizado mediante fuerza bruta.
* Al variar el tamaño de la clave, los resultados de frecuencias cambian aumentando el número de frecuencias de una letra en específico, lo cual puede facilitar para determinar que caracteres fueron usados para la clave.
* Es posible determinar la clave de usada en un algoritmo de encriptación mediante el análisis de sus frecuencias.
* El método de kasiski que consigue las triadas y sus frecuencias en los textos encriptados facilita el calculo de el criptoanálisis.
* Los métodos de sustitución y transposición de caracteres son eficientes a la hora de encriptar un texto, pero es fácilmente vulnerable al criptoanalis.
* Trabajando con un abecedario con mas caracteres, la fuerza del encriptado es mayor.

1. **CUESTIONARIO FINAL**
2. Trabajando en módulo 191 (un subconjunto imprimible del código ASCII del software Criptoclásicos), cifra el siguiente texto en claro con la clave: El ingenioso hidalgo.

*En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor. Una olla de algo más vaca que carnero, salpicón las más noches, duelos y quebrantos los sábados, lentejas los viernes, algún palomino de añadidura los domingos, consumían las tres partes de su hacienda. El resto della concluían sayo de velarte, calzas de velludo para las fiestas con sus pantuflos de lo mismo, los días de entre semana se honraba con su vellori de lo más fino. Tenía en su casa una ama que pasaba de los cuarenta, y una sobrina que no llegaba a los veinte, y un mozo de campo y plaza, que así ensillaba el rocín como tomaba la podadera.*

1. Descifre el criptograma en el mismo software ¿Por qué crees que el software no permite hacer un criptoanálisis?
2. Si el cifrado de Vigenere es IZLQOD y la clave SOL, ¿cuál era el mensaje en claro?
3. ¿Cuál será la cifra con autoclave del texto HABIA UNA VEZ, con la clave CIRCO?
4. En el ataque a Vigenere por Kasiski ¿Qué buscamos preferentemente?
5. Encontradas las cadenas repetidas en el criptograma, con separación d1, d2, d3 y d4 ¿Cuál sería la longitud L de la clave?
6. Si las distancias entre repeticiones de cadenas en un criptograma son 35, 112, 70. ¿Cuál sería la longitud L de la clave?
7. ¿Qué diferencia la regla AEOS de AEO en Kasiski?

**BIBLIOGRAFÍA**