Lab 1 – Encriptado y Decriptado de Texto

Competencias a desarrollar

- Implementar el uso de funciones para encriptar y decriptar un texto cifrado
- Identifica los requisitos para un análisis de fuerza bruta por frecuencia.

Problemas a resolver

1. Implementar las funciónes de encriptado y decriptado para un texto plano en castellano (27 letras) para los siguntes métodos (30 puntos)
    a. Cifrado Caesar

```
$ python caesar.py

Cifrado Cesar
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 1
Ingrese el texto a encriptar: hola como te encuentras hoy?
Ingrese el corrimiento: 3
Texto encriptado: krod frpr wh hqfxhqwudv kra?

Cifrado Cesar
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 2
Ingrese el texto a desencriptar:  krod frpr wh hqfxhqwudv kra?
Ingrese el corrimiento: 3
Texto desencriptado:  hola como te encuentras hoy?
```

    b. Cifrado afín

```
Cifrado Afin
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 1
Ingrese el texto a encriptar: buenos dias!
Ingrese el valor de a: 7
Ingrese el valor de b: 3
Texto encriptado: koenab xfdb!

Cifrado Afin
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 2
Ingrese el texto a desencriptar: koenab xfdb!
Ingrese el valor de a: 7
Ingrese el valor de b: 3
Texto desencriptado: buenos dias!
```

c. Cifrado Vigenére

```
$ python vigenere.py

Cifrado Vigenere
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 1
Ingrese el texto a encriptar: atacar al amanecer
Ingrese la clave: cypher
Texto encriptado: crpjej ya edcltjij

Cifrado Vigenere
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 2
Ingrese el texto a desencriptar: crpjej ya edcltjij
Ingrese la clave: cypher
Texto desencriptado: atacar al amanecer
```

2. Implementar el uso de funciones para encriptar y decriptar un texto cifrado. (30 puntos)

   Sugerencias:

   - Para construir una función que calcule las distribución de los caracteres que aparecen en el texto cifrado, se espera que su la función calcule las probabilidades **(las frecuencias divido el total de caracteres)**. (Es recomendable completar las letras que no aparezcan en su texto, con probabilidad 0.)

   Cesar

```
Ingrese el texto a encriptar: hola como estas?
Ingrese el corrimiento: 3
Texto encriptado: krñd fror hvwdv?
Distribucion de caracteres:
+-------+------------+
| Letra | Frecuencia |
+-------+------------+
|   a   |    0.00    |
|   b   |    0.00    |
|   c   |    0.00    |
|   d   |   15.38    |
|   e   |    0.00    |
|   f   |    7.69    |
|   g   |    0.00    |
|   h   |    7.69    |
|   i   |    0.00    |
|   j   |    0.00    |
|   k   |    7.69    |
|   l   |    0.00    |
|   m   |    0.00    |
|   n   |    0.00    |
|   ñ   |    7.69    |
|   o   |    7.69    |
|   p   |    0.00    |
|   q   |    0.00    |
|   r   |   23.08    |
|   s   |    0.00    |
|   t   |    0.00    |
|   u   |    0.00    |
|   v   |   15.38    |
|   w   |    7.69    |
|   x   |    0.00    |
|   y   |    0.00    |
|   z   |    0.00    |
+-------+------------+
```

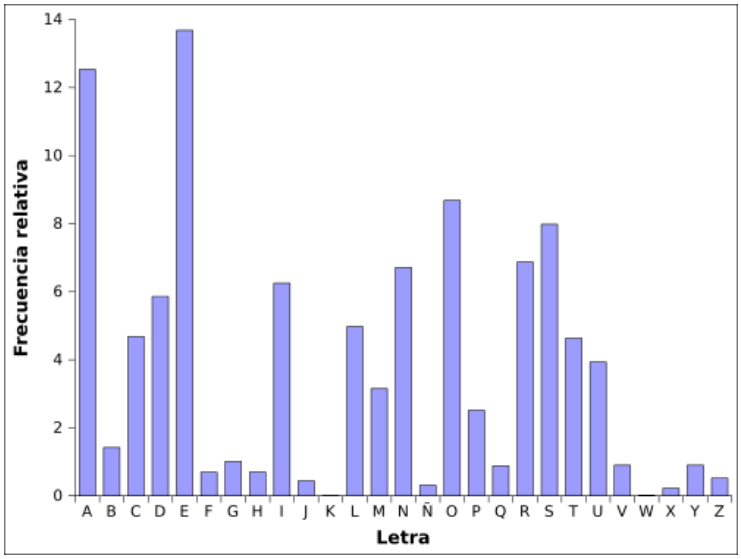
Afin

```
Ingrese una opcion: 1
Ingrese el texto a encriptar: hola como estas?
Ingrese el valor de a: 7
Ingrese el valor de b: 3
Texto encriptado: yazd qaga ebidb?
Distribucion de caracteres:
+-------+------------+
| Letra | Frecuencia |
+-------+------------+
|   a   |   23.08    |
|   b   |   15.38    |
|   c   |    0.00    |
|   d   |   15.38    |
|   e   |    7.69    |
|   f   |    0.00    |
|   g   |    7.69    |
|   h   |    0.00    |
|   i   |    7.69    |
|   j   |    0.00    |
|   k   |    0.00    |
|   l   |    0.00    |
|   m   |    0.00    |
|   n   |    0.00    |
|   ñ   |    0.00    |
|   o   |    0.00    |
|   p   |    0.00    |
|   q   |    7.69    |
|   r   |    0.00    |
|   s   |    0.00    |
|   t   |    0.00    |
|   u   |    0.00    |
|   v   |    0.00    |
|   w   |    0.00    |
|   x   |    0.00    |
|   y   |    7.69    |
|   z   |    7.69    |
+-------+------------+
```

Vigenere

```
Cifrado Vigenere
1. Encriptar texto
2. Desencriptar texto
3. Salir
Ingrese una opcion: 1
Ingrese el texto a encriptar: hola como estas?
Ingrese la clave: cypher
Texto encriptado: jnah tqke ikvyi?
Distribucion de caracteres:
+-------+------------+
| Letra | Frecuencia |
+-------+------------+
|   a   |    7.69    |
|   b   |    0.00    |
|   c   |    0.00    |
|   d   |    0.00    |
|   e   |    7.69    |
|   f   |    0.00    |
|   g   |    0.00    |
|   h   |    7.69    |
|   i   |   15.38    |
|   j   |    7.69    |
|   k   |   15.38    |
|   l   |    0.00    |
|   m   |    0.00    |
|   n   |    7.69    |
|   ñ   |    0.00    |
|   o   |    0.00    |
|   p   |    0.00    |
|   q   |    7.69    |
|   r   |    0.00    |
|   s   |    0.00    |
|   t   |    7.69    |
|   u   |    0.00    |
|   v   |    7.69    |
|   w   |    0.00    |
|   x   |    0.00    |
|   y   |    7.69    |
|   z   |    0.00    |
```

3. Implementar una función para comparar la distribución encontrada contra la distribución teórica de las letras del castellanos. (40 puntos)



Letra	A	B	C	D	E	F	G	H	I
Porcentaje	**12,53%**	**1,42%**	**4,68%**	**5,86%**	**13,68%**	**0,69%**	**1,01%**	**0,70%**	**6,25%**

Letra	J	K	L	M	N	Ñ	O	P	Q
Porcentaje	**0,44%**	**0,02%**	**4,97%**	**3,15%**	**6,71%**	**0,31%**	**8,68%**	**2,51%**	**0,88%**

Letra	R	S	T	U	V	W	X	Y	Z
Porcentaje	**6,87%**	**7,98%**	**4,63%**	**3,93%**	**0,90%**	**0,01%**	**0,22%**	**0,90%**	**0,52%**

Caesar corrimiento de 3

Comparacion con distribucion de caracteres en español:

Letra	Frecuencia	Frecuencia español
a	0.00	12.53
b	3.33	1.42
c	0.00	4.68
d	10.00	5.86
e	0.00	13.68
f	6.67	0.69
g	6.67	1.01
h	16.67	0.70
i	0.00	6.25
j	0.00	0.44
k	6.67	0.02
l	3.33	4.97
m	0.00	3.15
n	0.00	6.71
ñ	6.67	0.31
o	3.33	8.68
p	6.67	2.51
q	0.00	0.88
r	13.33	6.87
s	0.00	7.98
t	0.00	4.63
u	3.33	3.93
v	3.33	0.90
w	6.67	0.02
x	3.33	0.22
y	0.00	0.90
z	0.00	0.52

Mensaje: hola como te encuentras el día de hoy?
Mensaje encriptado: krñd fror wh hpfxhpwudv hñ gld gh krb?

En esta comparación de distribución de frecuencia se puede observar claramente un patrón en la distribución del texto cifrado, en donde justamente 3 posiciones delante de una letra con un porcentaje alto en la distribución teórica, se encuentra un porcentaje alto para la letra correspondiente al cifrado, este probablemente es en el cifrado donde se pueda observar de una manera más sencilla este patrón debido a la simpleza del cifrado cesar.

Afin con a = 7; b = 3

Comparacion con distribucion de caracteres en español:

Letra	Frecuencia	Frecuencia español
a	13.33	12.53
b	3.33	1.42
c	0.00	4.68
d	10.00	5.86
e	16.67	13.68
f	3.33	0.69
g	3.33	1.01
h	0.00	0.70
i	6.67	6.25
j	0.00	0.44
k	0.00	0.02
l	0.00	4.97
m	0.00	3.15
n	6.67	6.71
ñ	0.00	0.31
o	3.33	8.68
p	3.33	2.51
q	6.67	0.88
r	0.00	6.87
s	0.00	7.98
t	0.00	4.63
u	3.33	3.93
v	0.00	0.90
w	0.00	0.02
x	6.67	0.22
y	6.67	0.90
z	6.67	0.52

Mensaje: hola como te encuentras el dia de hoy?
Mensaje encriptado: yazd qaga ie enqoeniudb ez xfd xe yap?

En este cifrado se logra observar una distribución con un patrón que podría parecer a primera vista menos obvio, sin embargo, sabiendo que los porcentajes de que aparezcan ciertas letras son tan altos en las posiciones a, d y e esto nos da a entender que estas pueden representar algunas de las letras que mas se repiten en la distribución del castellano, lo cual lo hace una posible vulnerabilidad.

Vigenere con clave “cypher”

Comparacion con distribucion de caracteres en español:

Letra	Frecuencia	Frecuencia español
a	6.67	12.53
b	3.33	1.42
c	6.67	4.68
d	0.00	5.86
e	3.33	13.68
f	0.00	0.69
g	6.67	1.01
h	10.00	0.70
i	0.00	6.25
j	10.00	0.44
k	6.67	0.02
l	3.33	4.97
m	3.33	3.15
n	3.33	6.71
ñ	0.00	0.31
o	3.33	8.68
p	0.00	2.51
q	3.33	0.88
r	6.67	6.87
s	0.00	7.98
t	6.67	4.63
u	0.00	3.93
v	6.67	0.90
w	3.33	0.02
x	3.33	0.22
y	3.33	0.90
z	0.00	0.52

Mensaje: hola como te encuentras el dia de hoy?
Mensaje encriptado: jnah tqke xv ccjyvorhhw gj kmr bt lga?

En este cifrado se puede observar una distribución de letras mucho mas complicada de leer a comparación de las dos anteriores, debido a que estas se encuentran distribuidas mas uniformemente, lo que podría hacer la realización de un criptoanálisis mucho mas complicada. Por lo que se podría decir que el cifrado vigenere es el mas seguro de estos tres en cuanto a el estudio de las distribuciones de letras se refiere.