UNIVERSIDAD DEL VALLE DE GUATEMALA

Cifrado de información

Sección 10

Ludwing Cano

Laboratorio 1

Parte A

Abner Iván García Alegría 21285

Problemas a resolver

1. Implementar las funciones de encriptado y desencriptado para un texto plano en castellano (27 letras) para los siguientes métodos (30 puntos)

a. Cifrado Caesar

b. Cifrado afín

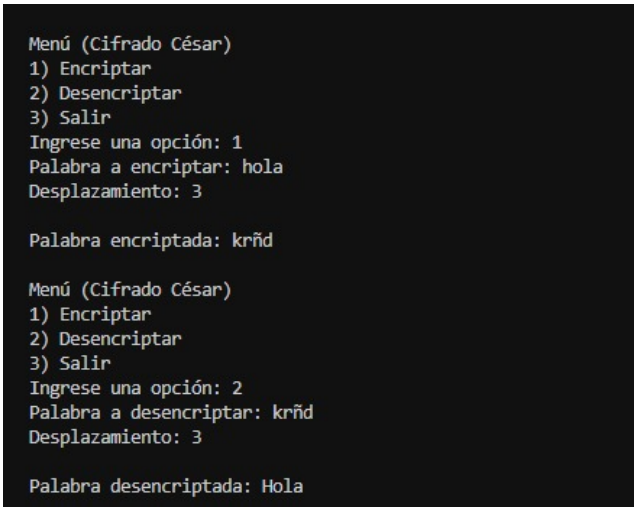
c. Cifrado Vigenere

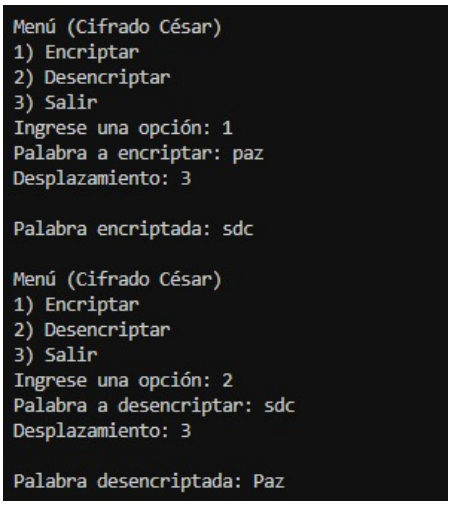
Para cada método, muestra ejemplos sencillos de encriptado y desencriptado (para verificar que funcionan correctamente).

Sugerencia:

- Para implementar funciones para encriptar y decriptar probablemente antes se deba construir una función que limpie el texto plano, removiendo caracteres no alfabéticos.

Cifrado Caesar





R// En este código primero se normaliza el texto eliminando acentos y convirtiéndolo en minúsculas. Luego, para cifrar, se toma cada letra del mensaje, se busca su posición en el alfabeto y se reemplaza por la letra que se encuentra un número de posiciones adelante según el desplazamiento dado. Para descifrar, el proceso es inverso: se retrocede en el alfabeto según el mismo desplazamiento. Caracteres que no están en el alfabeto, como espacios o signos de puntuación, se mantienen sin cambios.

Cifrado Afín

```
--- Cifrado Afín ---
1. Encriptar
2. Desencriptar
3. Salir
Seleccione una opción: 1
Ingrese el valor de 'a' (debe ser coprimo con 27): 11
Ingrese el valor de 'b': 7
Ingrese el mensaje: Mundo
Mensaje cifrado: evonk

--- Cifrado Afín ---
1. Encriptar
2. Desencriptar
3. Salir
Seleccione una opción: 2
Ingrese el valor de 'a' (debe ser coprimo con 27): 11
Ingrese el valor de 'b': 7
Ingrese el mensaje cifrado: evonk
Mensaje descifrado: mundo
```

```
--- Cifrado Afín ---
1. Encriptar
2. Desencriptar
3. Salir
Seleccione una opción: 1
Ingrese el valor de 'a' (debe ser coprimo con 27): 11
Ingrese el valor de 'b': 7
Ingrese el mensaje: mama
Mensaje cifrado: eheh

--- Cifrado Afín ---
1. Encriptar
2. Desencriptar
3. Salir
Seleccione una opción: 2
Ingrese el valor de 'a' (debe ser coprimo con 27): 11
Ingrese el valor de 'b': 7
Ingrese el mensaje cifrado: eheh
Mensaje descifrado: mama
```

R// Lo que realice para este algoritmo fue que cada letra del mensaje se convierte en una posición numérica dentro del alfabeto español y se transforma usando la fórmula matemática $E(x) = (a \cdot x + b) mod 27$, donde a y b son claves elegidas por el usuario y a debe ser coprimo con 27 para garantizar la descifrabilidad. Para descifrar, se usa la inversa modular de a y se aplica la ecuación inversa D(x)=a −1 ⋅(x−b)mod27. Este cifrado es más seguro que el César, ya que introduce multiplicación, haciendo que cada letra se transforme de manera menos predecible.

Cifrado Vigenere

```
Menú (Cifrado Vigenere)

1) Encriptar
2) Desencriptar
3) Salir

Ingrese una opción: 1
Palabra a encriptar: mundo
Ingrese clave: limon

Palabra encriptada: xczrb

Menú (Cifrado Vigenere)

1) Encriptar
2) Desencriptar
3) Salir

Ingrese una opción: 2
Palabra a desencriptar: xczrb
Ingrese clave: limon

Palabra desencriptada: Mundo
```

```
Menú (Cifrado Vigenere)

1) Encriptar
2) Desencriptar
3) Salir

Ingrese una opción: 1
Palabra a encriptar: Hola mundo
Ingrese clave: oso

Palabra encriptada: vgzo aifrc

Menú (Cifrado Vigenere)

1) Encriptar
2) Desencriptar
3) Salir

Ingrese una opción: 2
Palabra a desencriptar: vgzo aifrc
Ingrese clave: oso

Palabra desencriptada: Hola mundo
```

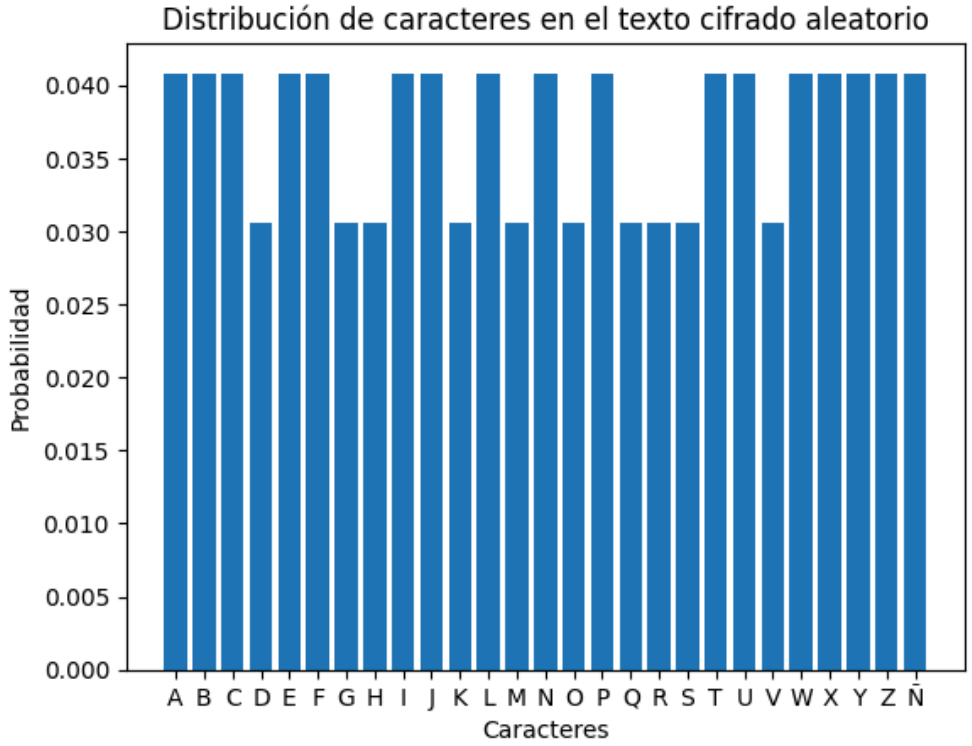
R// Para este utilizó una clave que se repite o se ajusta a la longitud del texto. Cada letra del mensaje es desplazada en el alfabeto según la posición de la letra correspondiente en la clave. Para descifrar, se invierte el proceso restando la posición de la clave. Este cifrado es más seguro que los cifrados monoalfabéticos, ya que la variabilidad del desplazamiento dificulta los ataques de frecuencia.

2. Implementar el uso de funciones para generar un análisis de frecuencia de un texto plano. (30 puntos)

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

```
Texto cifrado: FWLÑYEKRIADXNQUZBOHVJCTMSPGINXMUOQDAERGSKCFWYPLÑTVJHZBGZFEUYMOVDWPQAHJITRÑLKBNCXSPJAUZBC

Distribución en el texto cifrado aleatorio:
A: 0.041
B: 0.041
C: 0.041
D: 0.031
E: 0.041
F: 0.041
G: 0.031
H: 0.031
I: 0.041
J: 0.041
K: 0.031
L: 0.041
M: 0.031
N: 0.041
O: 0.031
P: 0.041
Q: 0.031
R: 0.031
S: 0.031
T: 0.041
U: 0.041
V: 0.031
...
X: 0.041
Y: 0.041
Z: 0.041
Ñ: 0.041
```

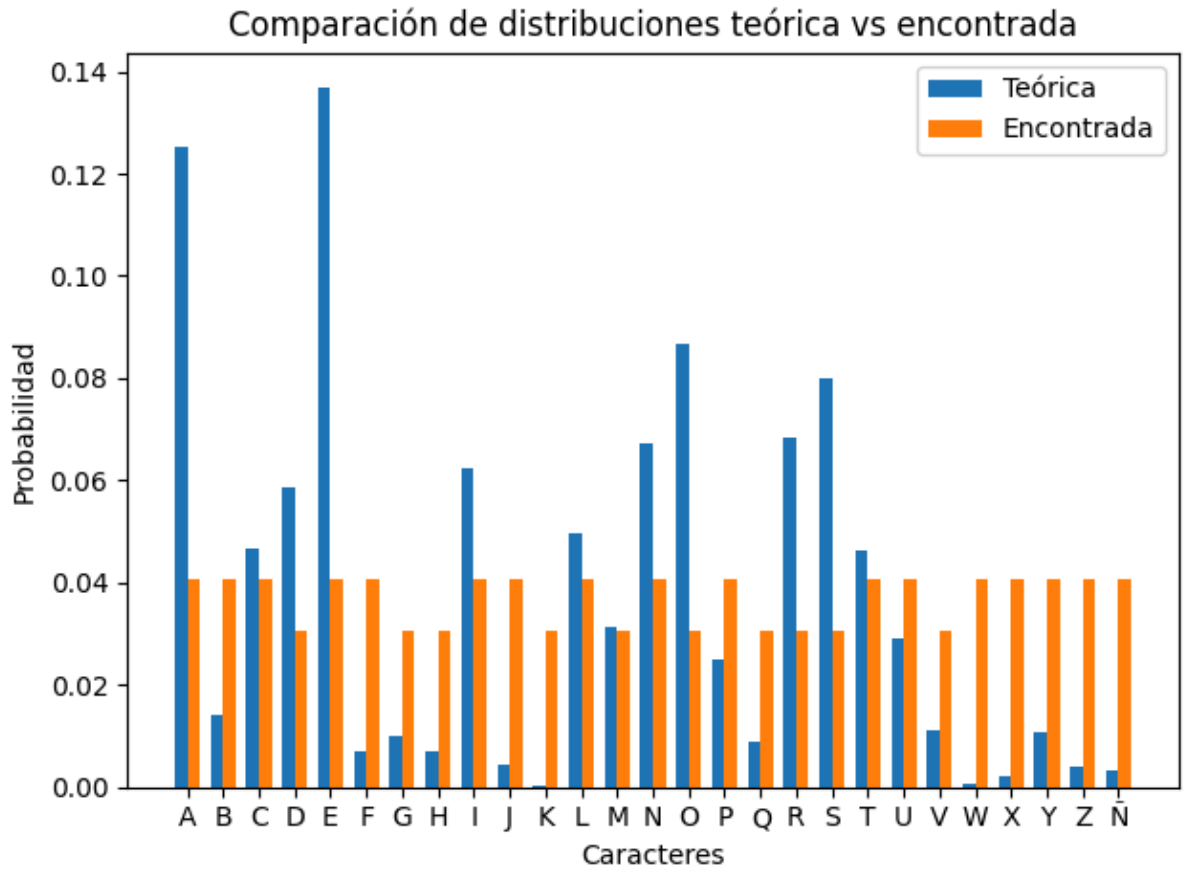


Se generó un texto aleatorio utilizando un cifrado que distribuye los caracteres de manera equitativa. Al calcular la frecuencia de aparición de cada letra en el texto resultante, se observa que la probabilidad de cada carácter se mantiene en torno a valores similares,

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

```python
# Distribución teórica de frecuencias de las letras en español brindadas en los docs
theoretical_distribution = {
    'A': 0.1253, 'B': 0.0142, 'C': 0.0468, 'D': 0.0586, 'E': 0.1368,
    'F': 0.0069, 'G': 0.0101, 'H': 0.0070, 'I': 0.0625, 'J': 0.0044,
    'K': 0.0002, 'L': 0.0497, 'M': 0.0315, 'N': 0.0671, 'Ñ': 0.0031,
    'O': 0.0868, 'P': 0.0251, 'Q': 0.0088, 'R': 0.0684, 'S': 0.0798,
    'T': 0.0463, 'U': 0.0291, 'V': 0.0111, 'W': 0.0008, 'X': 0.0021,
    'Y': 0.0108, 'Z': 0.0040
}
```

```
A: Teórica=0.1253, Encontrada=0.0408
B: Teórica=0.0142, Encontrada=0.0408
C: Teórica=0.0468, Encontrada=0.0408
D: Teórica=0.0586, Encontrada=0.0306
E: Teórica=0.1368, Encontrada=0.0408
F: Teórica=0.0069, Encontrada=0.0408
G: Teórica=0.0101, Encontrada=0.0306
H: Teórica=0.0070, Encontrada=0.0306
I: Teórica=0.0625, Encontrada=0.0408
J: Teórica=0.0044, Encontrada=0.0408
K: Teórica=0.0002, Encontrada=0.0306
L: Teórica=0.0497, Encontrada=0.0408
M: Teórica=0.0315, Encontrada=0.0306
N: Teórica=0.0671, Encontrada=0.0408
O: Teórica=0.0868, Encontrada=0.0306
P: Teórica=0.0251, Encontrada=0.0408
Q: Teórica=0.0088, Encontrada=0.0306
R: Teórica=0.0684, Encontrada=0.0306
S: Teórica=0.0798, Encontrada=0.0306
T: Teórica=0.0463, Encontrada=0.0408
U: Teórica=0.0291, Encontrada=0.0408
V: Teórica=0.0111, Encontrada=0.0306
W: Teórica=0.0008, Encontrada=0.0408
X: Teórica=0.0021, Encontrada=0.0408
Y: Teórica=0.0108, Encontrada=0.0408
Z: Teórica=0.0040, Encontrada=0.0408
Ñ: Teórica=0.0031, Encontrada=0.0408
```



R// Se realizó un análisis comparativo entre la distribución teórica de las letras en español y la distribución de frecuencias obtenida a partir de un texto cifrado aleatorio. La distribución teórica utilizada proviene de estudios previos sobre la frecuencia de aparición de las letras en el idioma español, mientras que la distribución encontrada se obtuvo a partir de un texto cifrado específico. Para realizar la comparación, se diseñó una función que toma ambas distribuciones y las presenta en forma de probabilidades para cada letra del alfabeto, incluyendo la letra Ñ. Los resultados muestran diferencias significativas entre ambas distribuciones, reflejando que en el texto cifrado las frecuencias de las letras están más uniformemente distribuidas en comparación con la distribución teórica, donde ciertas letras como la "A" y la "E" presentan una mayor frecuencia en el español natural.