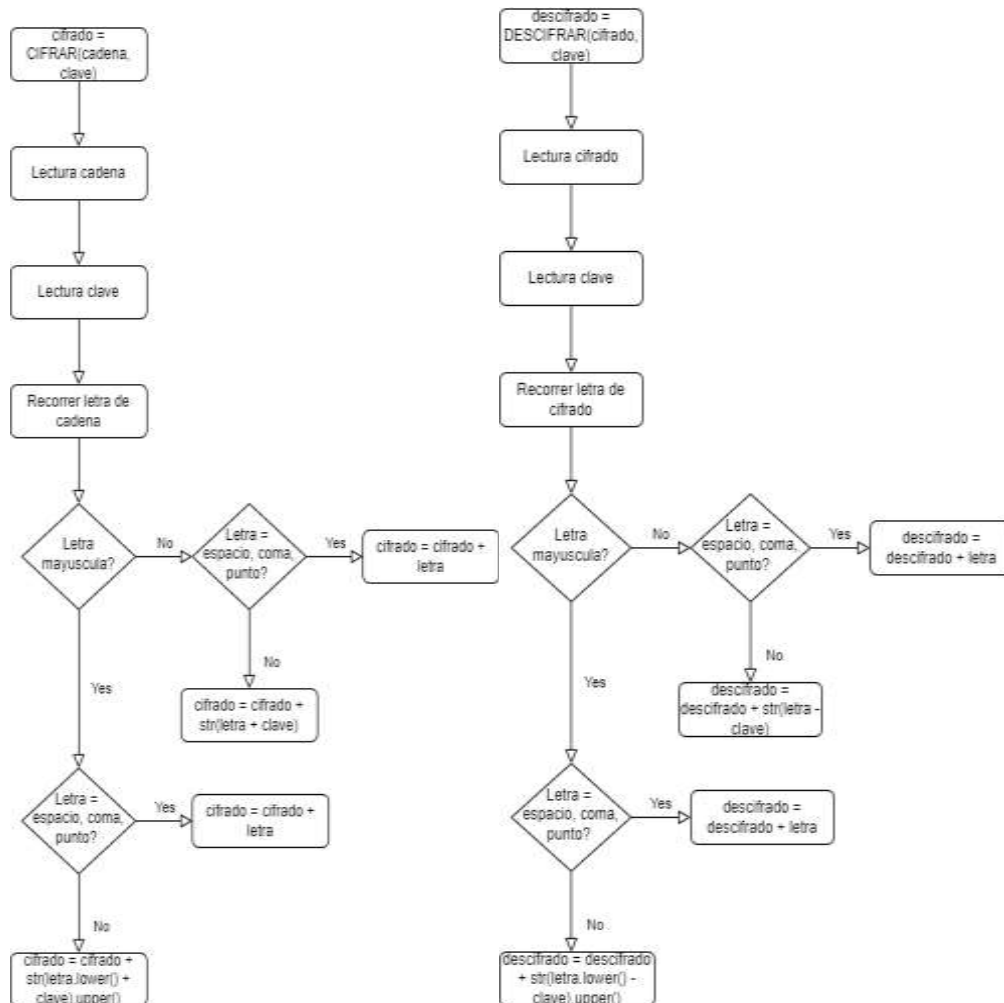


## PRÁCTICA 1. INTRODUCCIÓN AL LENGUAJE Y CIFRADO/DESCIFRADO VIGENÈRE

El primer paso para realizar el cifrado/descifrado vigenère es definir un diccionario, en este caso el del lenguaje castellano.

abc = 'abcdefghijklmnopqrstuvwxyz'

A continuación se deben definir tanto la función de cifrado como la de descifrado. En mi caso para definir dichas funciones he seguido los siguientes diagramas:



En el caso del cifrado, primero se realiza la apertura de los ficheros de entrada plain.txt y clave.txt, y a continuación se lee el contenido de dichos archivos. Se comienza recorriendo cada letra del texto a cifrar, mediante un bucle for. En cada una de las letras se mira si es mayúscula:

- Si es TRUE, se comprueba si dicha letra es un espacio, un punto o una coma:
  - o Si es TRUE: escribimos dicho carácter sin cifrar
  - o Si es FALSE: Le sumamos a la letra en minúsculas el correspondiente el carácter de la clave que le corresponde, es decir, ciframos. Y después pasamos a mayúscula dicho carácter.
- Si es FALSE, se comprueba si dicha clave es un espacio, un punto o una coma:
  - o Si es TRUE: escribimos dicho carácter sin cifrar

- Si es FALSE: Le sumamos a la letra el correspondiente el carácter de la clave que le corresponde, es decir, ciframos.

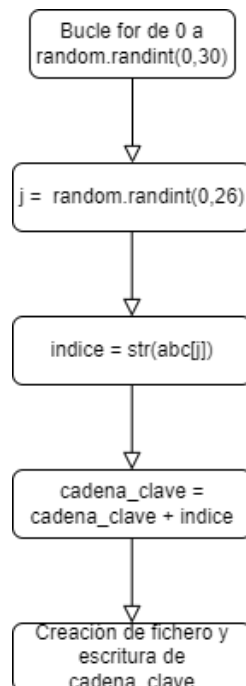
Por último, se escribe el texto cifrado en el archivo cifrado.txt, y se devuelve por pantalla la ruta donde se encuentra dicho archivo.

En el caso del descifrado, primero se realiza la apertura de los ficheros de entrada cifrado.txt y clave.txt, y a continuación se lee el contenido de dichos archivos. Se comienza recorriendo cada letra del texto a descifrar, es decir, el cifrado, mediante un bucle for. En cada una de las letras se mira si es mayúscula:

- Si es TRUE, se comprueba si dicha letra es un espacio, un punto o una coma:
  - Si es TRUE: escribimos dicho carácter sin cifrar
  - Si es FALSE: Le restamos a la letra en minúsculas el correspondiente el carácter de la clave que le corresponde, es decir, desciframos. Y después pasamos a mayúscula dicho carácter.
- Si es FALSE, se comprueba si dicha clave es un espacio, un punto o una coma:
  - Si es TRUE: escribimos dicho carácter sin cifrar
  - Si es FALSE: Le restamos a la letra el correspondiente el carácter de la clave que le corresponde, es decir, desciframos.

Por último, se escribe el texto descifrado en el archivo descifrado.txt, y se devuelve por pantalla la ruta donde se encuentra dicho archivo.

Hay que mencionar que la generación de clave se realiza de manera aleatoria para posteriormente escribir dicha clave en el fichero correspondiente. Para definir dicha función he seguido el siguiente diagrama:



En este diagrama se muestra que primero se realiza un bucle for para la definición de la longitud de la clave, y a continuación se realiza una asignación aleatoria para definir el carácter

de la clave. Después se va concatenando la cadena existente al nuevo carácter y por último en un fichero “clave.txt” se escribe dicha clave.

Por lo tanto el programa principal quedaría de la siguiente manera:

```
def main():  
    print(clave())  
    print(cifrar("plain.txt","clave.txt"))  
    print(descifrar("cifrado.txt","clave.txt"))  
  
if __name__ == '__main__':  
    main()
```

Por lo tanto, para ejecutar el programa únicamente es necesario un fichero “plain.txt” en el mismo directorio que el fichero fuente y una vez ejecutado se crearán los ficheros “cifrado.txt”, “descifrado.txt” y “clave.txt”.