1. Implementación de algoritmos de encriptado:

Cifrados por sustitución

Un **cifrado por sustitución** es un método de cifrado por el que unidades del texto original son sustituidas con texto cifrado siguiendo un sistema regular; las "unidades" pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros. El receptor descifra el texto realizando la sustitución inversa.

Compárese con los **cifrados por transposición**, en los que las unidades del texto original son cambiadas usando una ordenación diferente y normalmente bastante compleja, pero las unidades en sí mismas no son modificadas. Por el contrario, en un cifrado por sustitución, las unidades del texto plano mantienen el mismo orden, lo que hace es sustituir las propias unidades del texto original.

Sustitución simple

En los cifrados de **sustitución simple** un carácter en el texto original es reemplazado por un carácter determinado del alfabeto de sustitución. Es decir, se establecen parejas de caracteres donde el segundo elemento de la pareja establece el carácter que sustituye al primer elemento de la pareja.

Definir las funciones:

1. Generar un alfabeto común para el emisor y el receptor del mensaje que consistirá en las letra mayúsculas, minúsculas, números y espacio en blanco.

2. Implementar las funciones codifica letra (devuelve la posición del carácter en el alfabeto) y decodifica letra (recibe la posición que ocupa el carácter y devuelve el carácter).

3. Apoyándonos en las anteriores codificar cadena y decodificar cadena. La primera recibe una cadena de texto y devuelve una lista con las posiciones de cada letra y la otra al revés.

Cifrado de César

El ejemplo más sencillo de cifrado de sustitución simple es el cifrado de César. El cifrado César, con clave k, utiliza Tk(j)=(j+k)modL, como biyección en el conjunto de caracteres del alfabeto (estrictamente, en el conjunto de índices), con L el cardinal de dicho conjunto. En términos de índices, se usa la permutación:

$$(0,1,2,...,L-1)\mapsto(k,k+1,...,L-1,0,1,2,...,k-1).$$

4. Definir una función python, cifradoCesar(texto,clave,alfabeto), que espere un texto y una clave, y considere el anterior como alfabeto por defecto. La función devolverá el texto cambiando cada carácter por el que en el alfabeto ocupa k posiciones a su derecha (si el alfabeto se queda corto, se vuelve a empezar). Así cifradoCesar('Calzado',5) devolverá 'HfpDfit'. (Depende del orden de las letras en el alfabeto)