Informe preliminar

Contextualización:

En el desafío se nos propone desencriptar un texto contenido en un archivo, el cual esta encriptado de la siguiente manera:

1. Compresión; la cual puede ser de 2 tipos:

-RLE

- LZ78

2. Rotación de bits hacia a la izquierda

3. Operación XOR con clave de un byte

Análisis:

Tras entender el problema a solucionar debemos tener en cuenta que hay un árbol gigante de posibles caminos a seguir para solucionar este problema, debido a que, tenemos 2 posibles tipos de compresión, 8 posibles rotaciones de bits y 2^8 posibles claves XOR, llegué a la conclusión de que se debe implementar un código de fuerza bruta el cual evalué todas las posibles desencriptaciones hasta encontrar la correcta.

Diseño:

Para el diseño de este código, aunque estemos pensando en implementar un código de fuerza bruta debemos optimizarlo lo suficiente para así no hacer excesivos procedimientos más de la cuenta, por lo tanto, nos debemos apoyar contundentemente en la pista que se nos entrega (la entrada del programa es el mensaje encriptado y un fragmento del mensaje original el cual llamamos pista).

Tras esta primera semana de análisis, por ahora he llegado a la conclusión de que seria mas viable intentar encriptar la pista de todas las maneras posibles para así buscarla en el texto original encriptado hasta encontrar el que coincide.