Desafio 1

Juan pablo rivero garay

Posible solucionamiento del desafio por funciones que debe cumplir el código.

Paso a paso

**Compresión** (uno de los dos métodos):

**RLE (Run-Length Encoding)**: reemplaza secuencias repetidas por (cantidad + símbolo).

**LZ78**: usa un diccionario dinámico y pares (índice, caracter).

**Encriptación**:

**Rotación de bits** (izquierda, n posiciones, con 0 < n < 8).

**XOR con clave K (1 byte)**.(Ambos son reversibles.)

Posibles enfoques para resolver el desafío

1

Probar todas las combinaciones posibles de parámetros de encriptación (n y K) sobre el mensaje comprimido y verificar si, tras desencriptar y descomprimir, aparece el fragmento conocido.

Pasos:

* 1. Iterar valores de n en [1..7].
  2. Iterar valores de K en [0..255].
  3. Desencriptar el mensaje con cada combinación.
  4. Intentar descomprimir con RLE → verificar fragmento.
  5. Intentar descomprimir con LZ78 → verificar fragmento.

Hay que tener cuidado con la memoria

### **2**

### **Sincronización con el fragmento conocido**

En vez de desencriptar todo, usar directamente el **fragmento conocido** para inferir parámetros.

**Pasos:**

* 1. Tomar el fragmento conocido en binario.
  2. Compararlo con distintas ventanas del mensaje encriptado, aplicando la operación inversa parcial.
  3. Identificar el valor de n y K que lo hacen coincidir.

El problema es que si la pista no da la info posiblemente nos equivoc¿quemos

Conclusión

Vamos ha probar el primer método y en caso función tratar de mejorar la eficiencia y uso de memoria para evitar fugas