**DESAFIO 1**

**INFORMATICA II**

**REALIZADO POR:**

JUAN DIEGO ARBELAEZ MALPICA

SANTIAGO HENAO ZULUAGA

**UNIVERSIDAD DE ANTIOQUIA**

**ANALISIS DEL PROBLEMA**

**CONTEXTUALIZACION:**

* El cliente nos brinda un Dataset que contiene 4 textos planos que fueron comprimidos con (RLE o LZ78) y luego encriptados con (rotación de bits + XOR).
* Nuestras entradas serán:
  + Los mensajes comprimidos y encriptados.
  + Una pista por cada mensaje original.

**OBJETIVOS:**

1. Hallar:
   * Método de compresión usado (RLE o LZ78).
   * Valor de rotación de bits n.
   * Clave XOR K.
2. Desencriptar (desarrollar las operaciones inversas en el orden adecuado ).
3. Descomprimir el mensaje original y compararlo con el fragmento de pista dado.

**TENER EN CUENTA:**

* No utilizar librerías externas que ya resuelvan los métodos de compresión o encriptación.
* Optimizar lo que más se pueda la búsqueda del número de bits (n) y la clave (K) para no probar de forma innecesaria.
* Mantener el orden correcto de las operaciones inversas

**DIAGRAMA DE FLUJO**

Presentamos nuestro primer diagrama de flujo con el que pretendemos llegar a nuestra solución planteada. Teniendo en cuenta que está sujeto a modificaciones que se requieran para poder alcanzar nuestro objetivo.

DESCOMPRIMIR CON RLE

XOR CON K Y ROTAR n BITS A LA DERECHA

K = 0 a 255

0 < n < 8

LEEMOS TEXTO PLANO  
MENSAJE + PISTA

**¿PISTA ENCONTRADA?**

NO

SI

GUARDAR

DESCOMPRIMIR CON LZ78

¿**PISTA ENCONTRADA?**

TEXTO NO UTILIZA NINGUN METODO DE COMPRESION DADO

MOSTRAR TEXTO, n , K

GUARDAR

SI

NO