Preinforme - Practica 1 - informática 2

Introducción.

Este proyecto corresponde al Desafío 1 de la asignatura Informática II, cuyo propósito es simular un escenario de ingeniería inversa. A partir de un mensaje comprimido y encriptado, y conociendo únicamente un fragmento del texto original al que llamaremos “pista”, se busca identificar el método de compresión utilizado (RLE o LZ78), así como los parámetros de encriptación aplicados (rotación de bits y clave XOR). Posteriormente, se diseña e implementa un programa en C++ y utilizando la herramienta QTcreator para codificar dicho programa, que permita desencriptar y descomprimir el mensaje, logrando reconstruir el texto original que alguna vez fue comprimido y codificado.

Este reto pretende evaluar las habilidades adquiridas hasta esta instancia del curso, en particular el manejo de estructuras de control, punteros, arreglos, memoria dinámica y operaciones a nivel de bits. Al mismo tiempo, busca fortalecer la capacidad de análisis y resolución de problemas, enfrentando a los estudiantes a una situación que combina compresión de datos, encriptación y programación de bajo nivel en el lenguaje ya antes mencionado C++.

Análisis del problema

El desafío consiste en reconstruir un mensaje original en texto plano a partir de una versión comprimida y encriptada. El proceso aplicado para llegar al mensaje original tiene dos etapas:

1. Compresión: el texto inicialmente fue comprimido utilizando uno de dos algoritmos posibles:
   * RLE (Run-Length Encoding), el cual reemplaza secuencias de caracteres repetidos por pares (longitud, símbolo).
   * LZ78, el cual construye un diccionario dinámico de subcadenas y representa cada nueva secuencia como un par (índice, carácter).
2. Encriptación: el mensaje comprimido fue transformado mediante dos operaciones:
   * Una rotación de bits hacia la izquierda de cada byte en *n* posiciones, con 0 < n < 8.
   * Una operación XOR con una clave de un solo byte *K*.

El reto principal es que se desconoce tanto el método de compresión como los parámetros de encriptación (*n* y *K*). La única ayuda disponible es un fragmento conocido del mensaje original en un texto plano, que servirá como pista para validar los intentos de desencriptación y descompresión.

Entradas

* Cadena que contiene el mensaje comprimido y encriptado.
* Fragmento conocido del mensaje original (texto plano).

Salidas

* Mensaje original completo reconstruido en un archivo txt.
* Identificación del método de compresión utilizado (RLE o LZ78).
* Valores de los parámetros de encriptación: número de rotaciones (*n*) y clave XOR (*K*).

Dificultades principales

* Determinar de manera automática cuál de los dos algoritmos de compresión fue aplicado.
* Explorar el espacio de parámetros posibles de encriptación (7 posibles rotaciones × 256 posibles claves).
* Manejar estructuras de datos eficientes con punteros, arreglos y memoria dinámica, dado que no se permite el uso de librerías como string y estructuras STL
* Validar los resultados obtenidos comparando con el fragmento conocido del mensaje original.

Diseños analizados (Falta elegir el más conveniente)

Texto, Carta

El contenido generado por IA puede ser incorrecto.

Texto, Carta

El contenido generado por IA puede ser incorrecto.