Universidad de Antioquia

Facultad de Ingeniería

2570201: Informática II

Informe de análisis desafío 1

Luis Daniel González Correa

Ingeniería de Telecomunicaciones

Medellín, 2025

Universidad de Antioquia

Facultad de Ingeniería

2570201: Informática II

Informe de análisis desafío 1

Luis Daniel González Correa

Ingeniería de Telecomunicaciones

Dr. Augusto Enrique Salazar Jiménez

Medellín, 2025

Contexto de introducción

La empresa Informa2 recibió de un cliente un mensaje que fue sometido a un proceso de compresión y posteriormente encriptado. El reto consiste en diseñar un programa que permita recuperar el mensaje original a partir del archivo comprimido y encriptado, contando únicamente con un fragmento en texto plano como pista. En este contexto, es necesario considerar dos posibles métodos de compresión, RLE y LZ78, y un proceso de encriptación basado en la rotación de bits y la operación XOR. La solución debe ser capaz de identificar el método utilizado, los parámetros de encriptación empleados y, finalmente, reconstruir el texto original de manera completa.

Análisis

Para recuperar el texto original debo aplicar las operaciones inversas en orden XOR y rotación derecha, y luego descomprimir. La pista que se me brinda me permite enfocar la búsqueda. Pruebo con ambas descompresiones (RLE y LZ78). Si tras descomprimir aparece exactamente el fragmento conocido y los caracteres resultantes pertenecen al alfabeto permitido, considero que he identificado correctamente el método y los parámetros. La dificultad principal en términos prácticos es que LZ78 necesita crear un diccionario durante la descompresión, dado que no está permitido utilizar string ni STL, tengo que representar las cadenas del diccionario utilizando índices.

Solución preliminar

Al iniciar la ejecución, el programa pedirá al usuario cuántos archivos se van a evaluar. El número que el usuario ingrese (por ejemplo 4) define que el programa procesará los casos 1 a 4. Para cada índice i el programa leerá dos archivos con nombres fijos: Encriptado[i].txt y pista[i].txt con esos dos archivos intento identificar método y parámetros y se reconstruye el mensaje.

El flujo es que leo Encriptado[i].txt como un flujo binario de bytes y leo pista[i].txt como texto plano que contiene la pista conocida. Para buscar la solución pruebo los posibles valores de rotación n de 1 a 7 y la clave XOR K de 0 a 255. Para cada par aplico a una copia del buffer encriptado la operación inversa en el orden correcto: XOR con K sobre cada byte y luego rotación derecha por n. Con el buffer resultante intento descomprimirlo primero como RLE y si falla o no

contiene la pista, intento descomprimirlo como LZ78, si la descompresión tiene éxito y contiene la pista conocida, y además todos los caracteres de la salida pertenecen al alfabeto permitido, asumo que he identificado correctamente el método y los parámetros y guardo el resultado.

Resultado esperado

Para aceptar una solución para el caso i exijo dos condiciones:

1. Que la descompresión produzca una cadena que contenga exactamente la pista leída en pista[i].txt.

2. La cadena resultante solo contiene caracteres del conjunto permitido. Si ambos criterios se cumplen, se reporta el método y los parámetros y se termina el caso.

Si ambos métodos fallan, guardo un registro de que no lo encontré y analizo manualmente.