Preinforme desafío 1 informática 2

Por Michell Dayana Gaitan Gutierrez y Manuel José Montoya Arboleda

UdeA, facultad de ingenieria, 2025-2

Análisis del problema

Debemos crear un programa que desencripte y descomprima un mensaje cifrado utilizando loa algoritmos de descompresión RLE y LZ78, y de encriptación con rotación de bits y XOR con clave de manera inversa. Además, contamos con un fragmento del mensaje original a modo de pista.

Nuestra propuesta de solución es un programa que desencripta el mensaje con todas las posibles combinaciones de rotaciones y claves, conociendo que las rotaciones posibles son de 1 a 7 bits y las claves de 0 a 255. Para cada combinación de rotación y clave se ha de aplicar una verificación de validez del mensaje desencriptado y comprimido resultante, verificando que el primer carácter del mensaje sea un índice valido y basándonos en la cantidad de caracteres imprimibles presentes en el resultado (un mensaje comprimido valido debería tener una mayor cantidad de caracteres imprimibles que inválidos) para decidir si debe probarse o no la descompresión. Si se decide probar la descompresión para ese resultado, se hará un reconocimiento del patrón del mismo, para determinar a qué tipo de compresión pertenece su formato y aplicarla. Por último, se buscará que la pista coincida con algún fragmento del resultado, lo que validará si la combinación de pasos realizada corresponde con el proceso original aplicado al mensaje.

Planteamiento del programa

1. Función para lectura de los archivos y reserva en memoria de arreglos de char dinámicos para guardar el mensaje comprimido y encriptado y la pista del mensaje original.
2. Función de verificación de coincidencias, que genera los parámetros n, k, invoca funciones para cada algoritmo y detiene su ejecución cuando se detecte una coincidencia con la pista, para retornar los parámetros de esa combinación.
3. Función de encriptado inverso. Recibe los parámetros de la función de búsqueda para desencriptar el mensaje. El mensaje desencriptado se guarda en un arreglo dinámico de char, para liberarse en caso de que no se hallen coincidencias.
4. Función de compresión inversa. Una vez que la función de verificación considere valida una combinación de parámetros desencriptada y detecte un método de compresión, recibe el mensaje desencriptado y el método de

compresión, descomprime el mensaje con el algoritmo de compresión inversa correspondiente y retorna a la función de verificación el resultado. Este resultado se guarda también en un arreglo dinamico para eliminarse de ser necesario.