INFORME DESAFIO I

Jharlin Castro Moreno
Jharlin.castro@udea.edu.co

Mauricio Rafael Aguas Ramírez
mauricio.aguas@udea.edu.co

*Departamento de electrónica y telecomunicaciones, Faculta de ingeniería, UDEA, Medellín, Antioquia, Colombia

Resumen: Este informe presenta el análisis y diseño preliminar de una solución al Desafío 1 de la asignatura Informática II, cuyo objetivo es reconstruir un mensaje original a partir de su versión comprimida y encriptada. El proceso involucra identificar el método de compresión utilizado (RLE o LZ78), así como los parámetros de encriptación aplicados: rotación de bits y operación XOR. Se propone un enfoque modular que incluye las etapas de desencriptación, detección del algoritmo de compresión y descompresión, utilizando C++ con el framework Qt. El diseño considera las restricciones de no emplear estructuras de alto nivel como string o STL, privilegiando el uso de punteros, arreglos y memoria dinámica. Este pre-desarrollo constituye la base para la implementación final, la cual será validada mediante pruebas con un fragmento conocido del mensaje original.

Palabras claves: Compresión, RLE, LZ78, Encriptación, XOR, Rotación de bits, Ingeniería inversa.

Introducción

El presente informe corresponde a la etapa de pre-desarrollo del Desafío 1. El reto consiste en aplicar técnicas de ingeniería inversa para reconstruir un mensaje original que ha sido sometido a compresión y encriptación. El trabajo busca fortalecer las competencias de análisis, diseño y programación en C++, dentro de un entorno controlado pero cercano a situaciones reales.

Contextualización

El mensaje en texto plano fue sometido a dos transformaciones:

Compresión, utilizando uno de los algoritmos: RLE o LZ78.

Encriptación, mediante dos operaciones:

Rotación de bits hacia la izquierda en cada byte (n posiciones, $0 < n < 8$).

Operación XOR con una clave de un byte K.

El desafío consiste en recuperar el mensaje original, teniendo como única ayuda un fragmento conocido del mismo.

Análisis del problema

Entradas

- Mensaje comprimido y encriptado.
- Fragmento del mensaje original en texto plano.

Salidas

- Mensaje original completo.
- Método de compresión utilizado.
- Parámetros de encriptación: valor de rotación n y clave K.

Procesos principales

1. Identificación del método de compresión y de los parámetros de encriptación.
2. Desencriptación aplicando XOR inverso y rotación inversa.
3. Descompresión mediante RLE o LZ78.

Restricciones

- Implementación en C++ con Qt.
- No uso de objetos string ni STL.
- Uso obligatorio de punteros, arreglos y memoria dinámica.

Diseño propuesto

Esquema de tareas

1. Lectura de datos (mensaje encriptado y fragmento original).
2. Módulo de desencriptación (XOR inverso + rotación a la derecha).
3. Módulo de detección de compresión (prueba con RLE y LZ78).
4. Módulo de descompresión (RLE o LZ78 según corresponda).
5. Generación de la salida final (mensaje reconstruido y parámetros).

Módulo	Funciones Principales	Propósito
Validación Sintáctica	validar_sintaxis_lz78() validar_sintaxis_rle()	Verificar formato de datos desencriptados
Validación Semántica	validar_fragmento_conocido() buscar_subcadena()	Confirmar presencia del fragmento
Validación Integridad	validar_caracteres_permitidos() es_caracter_valido()	Verificar caracteres A-Z, a-z, 0-9
Desencriptación	desencriptar(), rotar_bits(), aplicar_xor()	Operaciones inversas de encriptación
Descompresión	descomprimir_rle() descomprimir_lz78()	Reconstruir texto original
Gestión Memoria	liberar_memoria() asignar_memoria()	Manejo eficiente de recursos

Algoritmos clave

- **Rotación de bits**: uso de desplazamientos y máscaras.
- **XOR**: operación bit a bit con la misma clave.
- **RLE**: conteo y expansión de secuencias repetidas.
- **LZ78**: diccionario dinámico con pares (índice, carácter).

Problemas potenciales

- Errores en el manejo de memoria dinámica y punteros.
- Complejidad en la implementación de LZ78 sin string ni STL.
- Dificultad en validar los parámetros n y K con certeza.
- Posibles desbordamientos en arrays o acceso indebido al diccionario.