## **Desafío 1 - Informática II**

### **1. Contextualización**

El desafío simula un escenario de ingeniería inversa donde se debe recuperar un mensaje original que ha sido sometido a procesos de compresión (RLE o LZ78) y encriptación (rotación de bits + XOR). El desafío consiste en:

**Entrada**:

Mensaje comprimido y encriptado

Fragmento conocido del mensaje original que nos sirve como única pista para la recuperación del mensaje.

**Proceso**:

Identificar el método de compresión utilizado

Determinar los parámetros de encriptación (n, K)

Aplicar las operaciones inversas en el orden correcto

**Salida**:

Mensaje original

Método de compresión y parámetros de encriptación.

### **2. Análisis del Problema**

#### **Algoritmos de compresión**

**-RLE**

**-LZ78**

#### **Encriptación**

La encriptación sigue dos operaciones reversibles:

1. **Rotación de bits** (n posiciones, 0 < n < 8)
2. **Operación XOR** con clave K (1 byte)

El espacio de búsqueda es manejable:

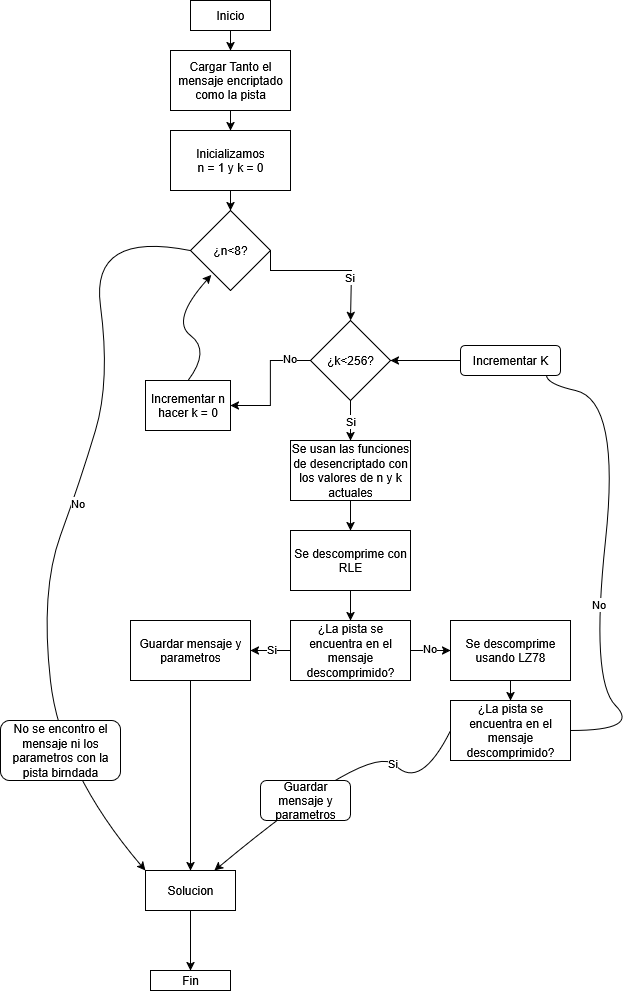
* 7 valores posibles para n (1-7)
* 256 valores posibles para K (0-255)
* Total: 1792 combinaciones posibles

#### **Solución**

1. Probar todas las combinaciones de n y K
2. Para cada combinación, aplicar desencriptación
3. Intentar descompresión con ambos algoritmos
4. Validar contra el fragmento conocido
5. Seleccionar la combinación que produzca coincidencia

### **3. Diseño de la Solución**

**Diagrama de flujo:**



**Enfoque Inicial:** El enfoque planificado consistía en desarrollar simultáneamente tanto el programa de compresión y encriptación como el de descompresión y desencriptación, construyendo progresivamente la complejidad de ambos sistemas. Se inició codificando los componentes básicos necesarios para el funcionamiento, implementando gradualmente funcionalidades adicionales en ambos programas para resolver el desafío. La meta era que, a medida que se incrementara la complejidad, se alcanzaría un punto donde el programa de desencriptado y descompresión coincidiría con los requerimientos del desafío.

**Cambio de Estrategia:** Este plan fue abandonado al identificar que los algoritmos que se pretendían implementar para la compresión RLE y LZ78 no coincidían con los utilizados en el dataset proporcionado. Sin embargo, no se anticipaban problemas con los componentes de encriptación/desencriptación.

**Nuevo Enfoque:** Se decidió entonces comenzar creando primero las funciones de desencriptación, tomando como referencia específica el archivo README.txt incluido en el dataset del proyecto.

**Funciones:** Se ha creado una carpeta de procesos que alberga programas auxiliares para el desarrollo del código principal. En particular, contiene dos programas dedicados a desencriptar ejemplos específicos del dataset de desarrollo. El objetivo de estos es identificar el formato de compresión utilizado, centrándose en los algoritmos RLE y LZ78.