**Informe Desafío 1-Informática 2**

Según los objetivos del desafío, este pretende evaluar la adquisición de los siguientes conocimientos en el estudiante: uso de estructuras de control (secuenciales, iterativas y condicionales), manejo de tipos de datos, operaciones a nivel de bits, punteros, arreglos, memoria dinámica y funciones. Es importante ser consiente y responsable sobre el dominio de estos temas para solucionar lo que se está pidiendo.  
  
Luego de realizar una lectura detallada del documento tome nota de las consideraciones iniciales, las cuales me brindaron conocimiento de forma didáctica acerca de los siguientes temas:

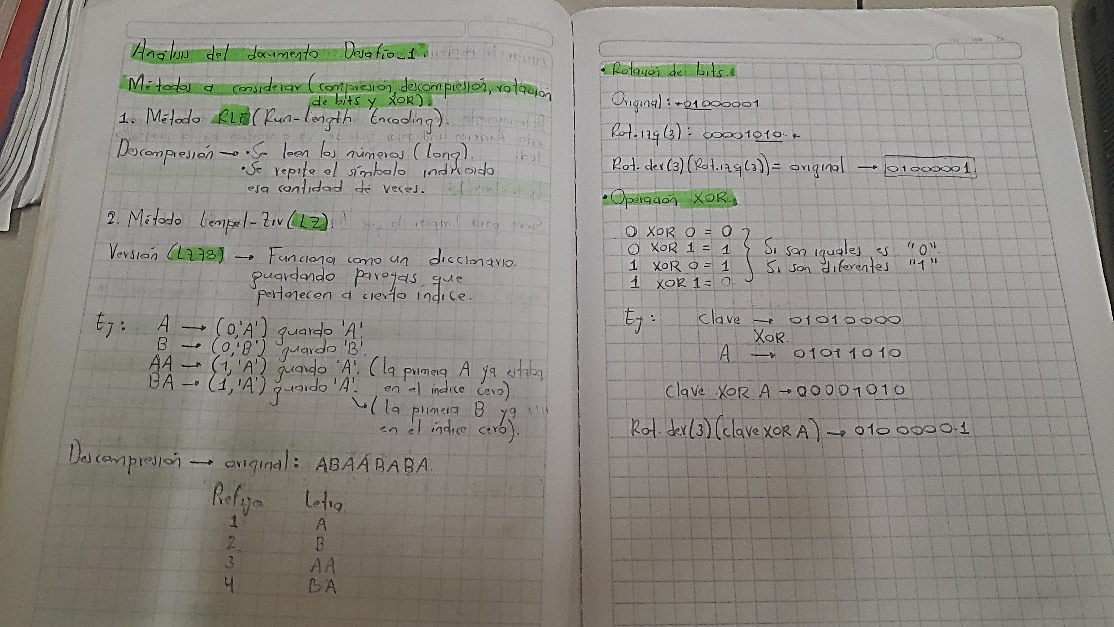
1. Métodos de compresión y descompresión RLE, LZ(LZ78)
2. Rotación de bits a la izquierda y derecha
3. Operación XOR

Al final del documento se explica de forma clara el problema a solucionar y de forma intuitiva puedo obtener un orden que como punto de partida puede ser fundamental para descifrar el código encriptado. Considero importante plasmar nuevamente ese orden:

1. El mensaje primero fue comprimido utilizando (RLE o LZ78)
2. Luego el mensaje es encriptado con dos operaciones consecutivas:

* Una rotación a la izquierda de cada byte en una cantidad n de bits (siendo 0 < n < 8).
* Una operación XOR con una clave de un solo byte K.

Nota: El texto dice consecutivas, sería probar cual fue primero que la otra

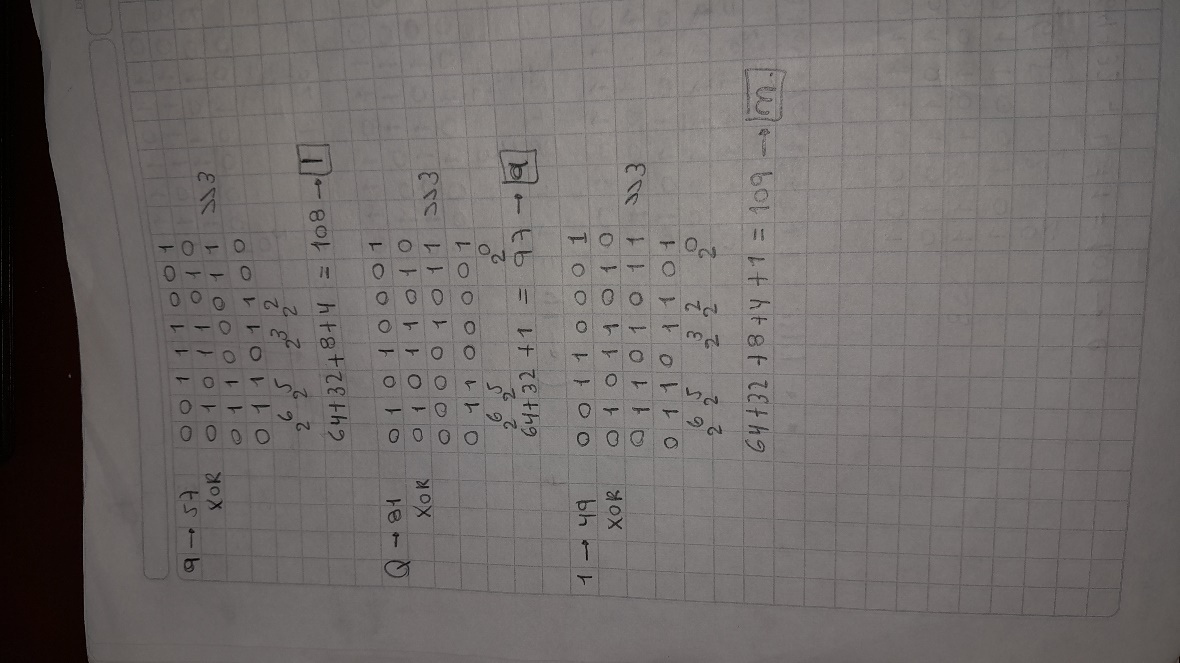
Importante: El desafío nos brinda un fragmento del texto transformado, el cual puedo utilizar para realizar cierta cantidad de pruebas teniendo en cuenta lo siguiente: la compresión puede ser RLE o LZ78, las dos operaciones consecutivas también me dan información; el número de bits rotados a la izquierda es un número entre 0 y 8 (1,2,3,4,5,6,7) y la operación XOR es una clave de 1 byte(8 bits).  
  
A continuación se comparte las imágenes del análisis manual del documento, con aspectos importantes para su comprensión y posteriormente inicio:

**Soluciones a los mensajes encriptados:**

**Análisis Encriptado1.txt:**

La comprensión de los pasos utilizados por el cliente para la encriptación del mensaje oculto que será descubierto por la empresa Informa2 se convierte en un recurso fundamental por lo siguiente:

* Los pasos para ocultar el mensaje nos dicen que hubo un orden: comprensión RLE o LZ78, luego se afirma que hubo rotación de bits a la izquierda en cada byte y seguidamente una operación XOR (no se sabe cuál se hizo primero de las dos).
* Al revisar el encriptado1.txt se observa que se repite un patrón (ZR), en donde concluyo que Z equivale 90 según la tabla ASCII y también equivale a 0x5A en hexadecimal (Z = 90 = 0x5A). Por otra parte, concluyo que R me indica que cada carácter tuvo una rotación de n bits y finalmente el carácter que está acompañando a el patrón repetitivo de ZR es el que sufrió la encriptación.
* Entonces aplicando las operaciones inversas para desencriptar cada carácter descubro que van siendo iguales a el mensaje original consecutivamente, cabe resaltar que en el README se indicaron los pasos para la encriptación y con base en esto se pudo realizar la operación o pasos inversos.
* Muy importante mencionar que este análisis se pudo desarrollar gracias a la aplicación de operaciones bitwise manualmente para una mejor comprensión y aprendizaje.



**Análisis Encriptado2.txt**

* Revisando el texto encriptado, mediante la observación me pude dar cuenta que también se repetía el mismo patrón de la Z, esta vez la Z estaba presente en cada tripleta, en algunas 2 veces repetidas y en otras solo una vez, pero nunca se repetía 3 veces.
* Al igual que el Encriptado1.txt asumí que la Z me estaba dando información acerca del XOR aplicado (0x5A = 90 = Z), pero a diferencia del primer encriptado la Z también me estaba indicando que letra o que pareja se estaba repitiendo, porque hay que recordar que en este problema se utilizó el método de compresión LZ78, entonces mediante unas pruebas manuales pude corroborar que:

1. Las tripletas me indican que cuando hay dos Z seguidas el tercer carácter no se repite, en cambio cuando la Z tiene otra letra distinta a ella en la segunda posición significa que esa letra ya estaba repetida, por ende, siguiendo la lógica de LZ78 esa letra repetida equivale a un índice a el cual le vamos a agregar una pareja (otra letra).
2. También pude corroborar que el primer índice repetido es igual a J, siguiendo la lógica de LZ78 el primer índice repetido es el “a”, entonces a ese índice repetido le agrego “n” = nuevo índice “an”.
3. Sabiendo eso y comprobando que coincide con el archivo Encriptado2.txt, surge una pregunta: **¿Qué operación oculta se aplicó para que el índice a sea igual a J?**
4. Después de realizar diferentes pruebas manuales con las operaciones bitwise descubrí que el segundo carácter de la tripleta diferente a Z es un índice, por ejemplo, al aplicar XOR a J con 0x5A y luego >>3 el resultado es 2, justamente en el índice 2 está la letra ‘a’, entonces la lógica del archivo encriptado va de esa manera.

**Análisis Encriptado3.txt**

* A diferencia del primer archivo encriptado, el cual también se comprimió utilizando RLE, en este archivo solo se repetía constantemente el patrón ‘@’ el cual inmediatamente busqué en la tabla ASCII y su valor correspondía a ‘64’ que también es igual a la semilla 0x40 en hexadecimal.
* Luego de saber esto, empecé a realizar varias pruebas manuales, pero el resultado no era lo esperado, hasta que me di cuenta que tenía un error con un solo bit en la conversión de la semilla a binario, lo cual me cambiaba todo el resultado.
* Finalmente descifré el siguiente orden: entre el primer y segundo término de cada tripleta apliqué XOR y posteriormente rotación de bits a la derecha >> 3, como resultado obtuve un número que me indica la cantidad de veces que esta repetida la letra, después hice el mismo procedimiento con el tercer término, manteniendo la misma semilla ‘@’y la rotación de bits a la derecha >>3, el resultado era la letra.

