Universidad Nacional Autónoma de México

Facultad de ciencias

Criptografía y Seguridad:

Práctica 01

Alex Gerardo Fernández Aguilar - 314338097

Angel Christian Pimentel Noriega - 316157995

Trabajo presentado como parte del curso de **Materia** impartido por el profesor **Prof** .

Archivo 1

Dado que vimos que el 1° y el 3° byte son iguales implica que su codificación debe ser la misma por esto concluimos que solo se ajusta a un formato JPEG sin embargo al realizar los calculo junto con la información de los primeros 2 bytes codificados y los 2 decodificados supuestos concluimos que las llaves provisionales para cifrar el archivo debieron ser $= \frac{37}{39}\, b = \frac{-2586}{13}$ sin embargo el 4° carácter no pudimos cifrarlo de forma que obtuviéramos el 4°byte que leíamos del archivo encriptado.

Archivo 2

En el archivo 2, probamos con cifrado César ya que mediante fuerza bruta obtuvimos todas las cabeceras de 5 bytes de el recorrido del archivo cifrado, después de esto revisamos en la terminal con *file ** el archivo de extensión de cada uno de los archivos , así revisamos y encontramos particularmente un *Audio file with ID3 version 2.4.0* es decir un **.mp3**. por lo cual pudimos con esto confirmar que era del corrimiento adecuado , revisamos el corrimiento y se realizo con 183 , por tanto como lo hicimos desde el archivo cifrado su llave deber ser $255 - 183 = 72$.
Adjuntamos el código utilizado para descifrar el archivo.

Archivo 3

En el archivo 3 al ser un archivo de tamaño pequeño sabemos que es un archivo de texto, utilizamos la página CyberChef, encontramos que en efecto el archivo 3 estaba codificado en Base 64.
El archivo dice: **FLAG{PRACTICA COMPLETADA!}**