Práctica 1
Criptografía y Seguridad

Fecha de entrega: 23 de Marzo de 2022.
No se reciben prácticas atrasadas después de esta fecha
Se puede entregar la práctica en a lo más equipos de 3.

1. Historia del problema

A tu amigo que le encanta andar descargando películas de internet vía BitTorrent fue descuidado y por accidente descargó un virus que al momento de abrir la película descargada, se ejecutó el virus haciendo que sus archivos en el directorio donde estaba el archivo fueran cifrados y como tú estudias en la Facultad de Ciencias, te ha pedido que si puedes ayudarle a restaurar sus archivos como estaban, él recuerda que se trataba de un archivo de texto, una canción y una imagen.

Tu amigo, para echarte un poco la mano, descubrió que los cifrados que utilizaron los programadores del virus son cifrados simétricos, es decir, es posible que se rompa el cifrado sin conocer la llave, ¿podrías ayudar a tu amigo? De otra manera él tendrá que pagar 1,000,000 bitcoins para recuperar sus archivos.

Piensa también en que el cifrado puede no necesariamente ser por el contenido de los archivos, si no a nivel de bytes, en cuyo caso cambia el tamaño de los alfabetos.

También necesitarás investigar el cifrado para cada uno de los archivos cifrados de tu amigo, de entre los cuales pueden ser: Cifrado césar, cifrado afín, cifrado Base64, cifrado de Vigenere.

2. Procedimiento

Descargar el repositorio público: https://github.com/FernandoFong/CyS-2022-2[1] Ahí encontrarás un directorio llamado `Practica1`, en este directorio hay 3 archivos con terminación `.enc`, el objetivo de esta práctica es descifrarlos como se pueda, sin embargo guarda el procedimiento que utilizaste para obtener los archivos descifrados.

3. Entregables

Lo mínimo para entregar en esta práctica para que sea evaluable es:

1. Un archivo (no necesariamente PDF) donde redacten el procedimiento que siguieron para desencriptar los archivos.
2. Los archivos desencriptados a manera de que tu amigo pueda volverlos a abrir como estaban.
3. Scripts auxiliares de cualquier lenguaje que les hayan ayudado a desencriptar estos archivos.

Por último, obtener la bandera de entre los archivos que tiene el formato: ****{******** **********!}

4. Formato de entrega

Subir todos los archivos comprimidos en extensión `.zip`, `.tar.gz` o `.7z`, en caso de que entreguen la práctica en equipos, deberán de agregar un README con los nombres de los integrantes y subirlo a la actividad del classroom, el 23 de Marzo antes de las 23:59:59.

[1] Conserva este repositorio puesto que será donde se subirán las prácticas de todo el curso.