Criptografía
Práctica SL4
Informe de prácticas

1. **Obtenga y/o genere fichero de texto, una imagen BMP, un fichero formado por datos aleatorios y un fichero formado por un único byte repetido y encripte y desencripte estos ficheros usando diferentes algoritmos (AES, DES, CAMELLIA, BLOWFISH) y diferentes modos de cifrado (ECB, CBC, CFB). Recopile cuantos resultados pueda de este proceso (memoria usada, tiempo necesario para encriptar y desencriptar,…). Muestre en una o varias tablas los resultados obtenidos (tiempos, tamaños,…) y coméntelos.**
   [SUS RESPUESTAS]

2. **Escriba un programa, en el lenguaje de programación que desee, que calcule la media aritmética de los bytes de un fichero.**
   [SUS RESPUESTAS]

3. **Comprima con *gzip* los cuatro ficheros usados en la cuestión 1. Usando el programa anterior, obtenga la media aritmética de los bytes que componen los cuatro ficheros usados en la cuestión 1, sus correspondientes archivos comprimidos y sus correspondientes archivos encriptados con AES-ECB, AES-CBC, DES-ECB y DES-CBC. Muestre los resultados en una tabla y coméntelos. ¿De qué puede ser un indicador la media aritmética de los bytes de un fichero?**
   [SUS RESPUESTAS]

4. **Escriba un programa, en el lenguaje de programación que desee, que calcule la entropía de la información de un fichero.**
   [SUS RESPUESTAS]

5. **Usando el programa anterior, obtenga la entropía de la información de los cuatro ficheros usados en la cuestión 1, sus correspondientes archivos comprimidos con *gzip* y sus correspondientes archivos encriptados con AES-ECB, AES-CBC, DES-ECB y DES-CBC. Muestre los resultados en una tabla y coméntelos. ¿Por qué $\mathcal{H}(X) \in [0,8]$? ¿Existe alguna relación entre la entropía, $\mathcal{H}(X)$, de los ficheros sin comprimir y el tamaño de los correspondientes ficheros comprimidos?**
   [SUS RESPUESTAS]

6. **Encripte la imagen *test.bmp* usando el algoritmo AES con los modos de cifrado ECB y CBC. Salve una copia de la imagen cifrada, copie la cabecera de 54 bytes de la imagen original en el fichero cifrado y muestre (corte y pegue en la respuesta) las tres imágenes. Comente y explique, a la luz de los resultados, por qué sucede esto.**
   [SUS RESPUESTAS]