Criptografía y Seguridad *(72.44)*

TRABAJO PRÁCTICO 1: CIFRADO POR BLOQUES

1. Objetivos

Experimentar con los algoritmos de cifrado por bloques, en particular AES y DES.

Analizar los resultados obtenidos al aplicar distintos modos de operación para algoritmos de cifrado por bloques.

2. Consigna

Realizar un programa en lenguaje C que, dada una imagen .BMP:

1) Encripte la imagen mediante algún algoritmo de cifrado por bloques, obteniendo una nueva imagen .BMP de las mismas dimensiones de la imagen original.
2) Desencripte la imagen, conocida la clave y IV o conocido el password, mediante algún algoritmo de cifrado por bloques, obteniendo una imagen .BMP.

3. Detalles del sistema

3.1. Encripcion – Desencripcion

El programa debe recibir como parámetros:

- **`-in`** imagen (en formato .bmp)
- **`-out`** imagen (en formato .bmp)
- **`-e (`**encripcion) o bien **`-d`** (desencripcion)
- **`-pass password`** (password de encripcion). O bien –K key –iv vectorInicializacion
- **`-a <aes | des>`**
- **`-m <ecb | cfb | ofb | cbc>`**

Ejemplo:

Encriptar la imagen “kitty.bmp” con aes en modo ecb, con password “hello” obteniendo como salida “kittyEnc.bmp”

```
$criptoImagenes –in “kitty.bmp” –out “kittyEnc.bmp” –e –pass “hello” –a aes –m ecb
```

3.2. Archivos .BMP

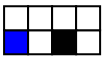
El formato BMP es un formato de archivos de imagen bastante simple. Consta de dos partes:

- encabezado → de 54 bytes
- Cuerpo → de tamaño variable.

El encabezado contiene información acerca del archivo: tamaño de archivo, ancho de imagen, alto de imagen, bits por píxel, si está comprimido, etc

IMPORTANTE: Considerar la versión V3 de archivos BMP. Es la más común. No hace falta considerar otras versiones que puedan tener otro tamaño y datos de encabezados.

En el cuerpo del archivo bmp, están los bits que definen la imagen propiamente dicha. La imagen se lee de abajo hacia arriba y de izquierda a derecha. Si la imagen es de 24 bits por píxel, la distribución es: 8 primeros bits para azul, 8 bits para verde, y 8 bits para rojo.



Ejemplo: La imagen de la izquierda representa un bmp de 4 pixeles por 2 pixeles. El primer píxel leido es el azul, luego el blanco, luego el negro.

Si la imagen es de 24 bits por píxel, el píxel azul tiene la siguiente estructura:

1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Lo que interesa para este trabajo práctico es encriptar y desencriptar los datos de la imagen propiamente dicha, sin ningún tipo de compresión. Las características tales como tamaño de la imagen, ancho, alto, deben mantenerse. Por eso los archivos encriptados también deberían poder visualizarse como cualquier otro .bmp.

IMPORTANTE: Considerar archivos que no estén comprimidos. Para ello, controlar el parámetro de compresión del encabezado que tiene la información de si la imagen fue comprimida con algún algoritmo (por ejemplo RLE)

3.3. Consideraciones generales.

- La imagen, siempre en formato bmp, podrá ser de 1 a 24 bits por píxel.
- El resultado de la encriptación **también es una imagen.bmp**, que conserva las dimensiones de la imagen original, y la misma paleta de colores.
- El algoritmo AES pueden considerarlo sólo con claves de 128 bits.
- Si la imagen no puede particionarse en bloques de igual tamaño para el cifrado pueden tener inconvenientes de acuerdo a cómo se efectúe el padding. Por lo tanto, pueden considerar descartar la imagen en caso de que la cantidad de bytes no sea múltiplo del tamaño de bloque.

4. Cuestiones a analizar.

Una vez obtenido el programa, deberán analizarse las siguientes cuestiones:

1. ¿Qué ocurre con las imágenes encriptadas con DES en modo ECB?
2. Repetir la encriptación con AES y comentar si la situación mejora o no.
3. Repetir la encriptación con DES y AES en modo CBC y analizar los resultados obtenidos.
4. Repetir la encriptación con DES y AES en modo CFB y analizar los resultados obtenidos.
5. ¿Qué ocurre al querer desencriptar una imagen con una clave incorrecta?
6. Encontrar una imagen que podría ser encriptada con cierta eficiencia usando un cifrado de bloque en modo ECB. Justifica la elección de la misma.

5. Organización de los grupos

El trabajo será realizado en grupos de 3 integrantes como máximo**. Para el 12 de abril** deberán dar a conocer los nombres de los integrantes de cada grupo y una dirección de email a la cátedra.´

Cada grupo recibirá, en la semana del 12 de abril, un par de imágenes de prueba.

6. Entrega

La fecha de entrega es el día 28 de abril.

Cada grupo entregará el ejecutable y el código en C, junto con la documentación correspondiente al uso del programa.

Además presentarán un informe con la solución correspondiente al descifrado de los archivos que se le entregaran oportunamente al grupo y con el análisis de las cuestiones planteadas en el punto 4.

7. Material de lectura recomendado

- **Capítulo 9 de Computer Security – Art and Science, Matt Bishop, Addison-Wesley, 2004**
- **Capítulo 7 de Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, CRC Press, 1997**