Teoría de la Información y Codificación

Práctica 7: Criptografía

José A. Montenegro Montes

26 de septiembre de 2014

1. Enunciado

El objetivo de la práctica es experimentar con un algoritmo de cifrado por bloques, concretamente DES. Para ello practicaremos el cifrado y descifrado con los distintos modos (ecb, cfb, ofb, cbc).

Los archivos que cifraremos/descifraremos serán imágenes BMP (Bitmap Image File)[1] sin ***comprimir***. Para el tratamiento de las imágenes BMP utilizaremos las clases de la Práctica anterior.

Para realizar la práctica, es necesario implementar el algoritmo del DES. A modo de ejemplo es posible utilizar el código del campus virtual que realiza una implementación incompleta del DES, donde es necesario incluir la opción de descifrado, que implica:

- Añadir desplazamiento a la derecha de los bits.
- Actualizar el proceso de subclaves.
- Añadir el método de descifrado y

La implementación del DES puede ser modificada para obtener un código más eficiente. Para verificar que el algoritmo del DES funciona correctamente es necesario utilizar la definición del estándar FIPS 46-2.

2. Evaluación

La ejecución de la aplicación, además de generar y visualizar las imagenes AndroidCifradoModo.bmp (imagen cifrada por DES utilizando uno de los modos) y AndroidDescifradoModo.bmp (imagen recuperada mediante el método descifrado del DES), mostrará por pantalla:

- Tiempo Cifrado: ECB → xx Nanosegundos, CFB → xx Nanosegundos, OFB → xx Nanosegundos, CBC → xx Nanosegundos.

[1] Wikipedia BMP

- Tiempo Descifrado: ECB → xx Nanosegundos, CFB → xx Nanosegundos, OFB → xx Nanosegundos, CBC → xx Nanosegundos.
- Diferencias archivos original y descomprimidos: Differencias **en bits** entre la imagen original y la obtenida tras descifar la imágen que **debe ser cero**. Para realizar la comparación es posible utilizar la clase $CompararImagenes.java$.

3. Conclusiones

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

1. Mostrar información comparativa (tiempo) de la implementación del DES realizada, con respecto a la implementación del DES aportada por la SDK de Java.
   - Tiempo Cifrado JAVA: ECB → xx Nanosegundos, CFB → xx Nanosegundos, OFB → xx Nanosegundos, CBC → xx Nanosegundos.
   - Tiempo Descifrado JAVA: ECB → xx Nanosegundos, CFB → xx Nanosegundos, OFB → xx Nanosegundos, CBC → xx Nanosegundos.
2. ¿Qué ocurre con las imágenes cifradas con DES en modo ECB?
3. Repetir el cifrado con DES en modo CBC y analizar los resultados obtenidos.
4. Repetir el cifrado DES en modo CFB y analizar los resultados obtenidos.
5. ¿Qué ocurre al querer descifrar una imagen con una clave incorrecta?