

# Criptografía y Seguridad

## Cifrado por Bloques

Domé, Damián

Bombau, Nicolás

Castro, Carlos

28 de abril de 2010

# Índice

<b>1. Introducción</b>	<b>3</b>
<b>2. Programa</b>	<b>3</b>
<b>3. Consideraciones y Validaciones</b>	<b>3</b>
<b>4. Análisis de los resultados</b>	<b>4</b>
4.1. DES y ECB . . . . .	4
4.2. AES y ECB . . . . .	4
4.3. DES y AES, con CBC y CFB . . . . .	5
4.4. Descripción con Clave Incorrecta . . . . .	5
4.5. Análisis ECB . . . . .	5
<b>5. Bibliografía</b>	<b>6</b>

## 1. Introducción

Se detallan a continuación los criterios de diseño e implementación programa que dada una imagen *bmp*, pueda encriptarla y desencriptarla mediante el uso de algoritmos de cifrado por bloques. Al encriptar una imagen, se obtendrá una nueva imagen de dimensiones iguales a las de la original. Para desencriptar la imagen, deberá conocerse el password, o la clave y el vector de inicialización, dependiendo del algoritmo.

## 2. Programa

El programa permite la encriptación y desencriptación de imágenes mediante DES y AES. Para cada una de estas primitivas, se puede optar por los métodos ECB, CBC, CFB y OFB.

El programa recibe los siguientes parámetros:

- -in imagen (en formato bmp)
- -out imagen (en formato bmp)
- -e (encriptación) o -d (desencriptación)
- -pass password o -K key -iv
- -a ( aes, des)
- -m (ecb, cfb, ofb, cbc)

Como las imágenes se encriptan sin ningún método de compresión, los archivos encriptados pueden visualizarse como cualquier otro bmp.

## 3. Consideraciones y Validaciones

Aquí se presentan las consideraciones generales respectivas a la implementación:

- La imagen, siempre en formato bmp, podrá ser de 1 a 24 bits por píxel
- El resultado de la encriptación es también una imagen bmp que conserva las dimensiones de la imagen original, y la misma paleta de colores
- El algoritmo AES se considera sólo con claves de 128 bits
- Si la cantidad de bytes de la imagen no es múltiplo del tamaño del bloque, se descartará la imagen
- Para el cifrado con feedback, se fija la cantidad de bits de feedback
- Se fijó la longitud del password, del key y del vector de inicialización. La longitud debe ser igual al tamaño del bloque del algoritmo a utilizar (8 para DES, 16 para AES)

## 4. Análisis de los resultados

Aquí se exponen algunos resultados obtenidos.

### 4.1. DES y ECB

Supongamos la siguiente imagen:



Figura 1: Tux

Al encriptarla con DES, se obtiene el siguiente resultado:



Figura 2: Tux con DES en modo ECB

Como se puede ver, en la imagen encriptada se observan claramente los contornos de la figura presente en la imagen sin encriptar.

Luego de hacer pruebas con varias imágenes, se dedujo que en las zonas que tienen cambios bruscos de colores, al encriptarse, dichos cambios siguen viéndose, pudiendo inferir la imagen sin encriptar.

Por otro lado, cuando las imágenes tienen transiciones mas paulatinas de color a color, el encriptado es mucho mejor.

### 4.2. AES y ECB

Al encriptar con AES y ECB, los resultados son muy similares a los de DES y ECB, pues los cambios bruscos de color también permanecen en la imagen encriptada.

### 4.3. DES y AES, con CBC y CFB

Al encriptar con los métodos CBC y CFB, ya sea con AES o DES, en todos los casos que se probó fue imposible inferir la imagen sin encriptar a partir de la imagen encriptada, para ninguna de las 4 combinaciones, es decir, todas arrojaron resultados igualmente buenos. En caso de utilizarlas en algún momento que se necesite encriptar imágenes, la decisión final dependería de las virtudes de cada uno de los métodos de encadenamiento. Con respecto al algoritmo, se elegiría AES, por una cuestión de que DES ya se considera quebrada.

Vemos ahora encriptación de la imagen anterior, utilizando AES y CBC:



Figura 3: Tux con AES en modo CBC

y, para comparar, la misma imagen encriptada utilizando DES y CFB:

### 4.4. Desencriptación con Clave Incorrecta

Supongamos que encriptamos una imagen con cualquier algoritmo (AES o DES) y con cualquier método (ECB, CBC, CFB o OFB). Si el password para encriptar fuese *hola* pero a la hora de desencriptar usamos *chau*, la imagen no puede ser recuperada.

### 4.5. Análisis ECB

Al encriptar la imagen del pinguino se vio que aún los rasgos del mismo eran visibles en la imagen encriptada. Sin embargo, como se dijo anteriormente, las imágenes que tienen cambios paulatinos de colores podrían ser más aptas para la encriptación con encadenamiento ECB.

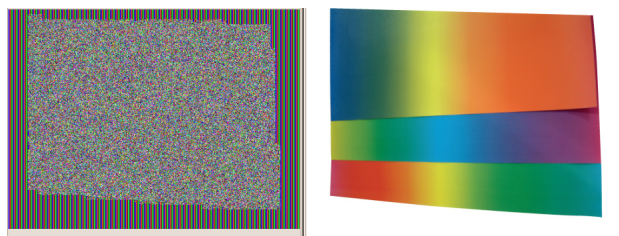


Figura 4: Degrade

Como se puede observar en la figura 4, los cambios graduales de la figura del centro de la imagen, no muestran un patrón reconocible en la versión encriptada. Sin embargo, en los bordes de la figura, el cambio brusco produce un traspaso de información en la imagen encriptada, donde se reconoce dicho cambio a simple vista.

## 5. Bibliografía

- Computer Security - Art and Science, Matt Bishop, Addison-Wesley, 2004
- Handbook of Applied Cryptography, Alfred Menezes, Paul Van Oorschot, Scott Vanstone, CRC Press, 1997