

AES Cipher Modes

Elegimos la imagen bmp:



Y la ciframos usando dos modos de operacion distintos:

ECB

Usamos el modo de operacion Electronic Code Book, es un metodo de poca carga para el procesador.

No es recomendado ya que no utiliza un vector de inicializacion, por lo que la salida siempre es la misma para la misma entrada.

La unica ventaja, es que el error en algun bloque no es propagable.

Comando:

```
openssl enc -aes-128-ecb -e -in secret.bmp -out Csecret.bmp -K 1001011 -iv 0010011
```

Donde:

- Se utiliza AES

- Con 128 bits como llave

- El archivo de entrada es secret.bmp

- La clave es 1001011 (tiene que especificarse en hexadecimal)

- Y el vector de inicializacion es 0010011

Despues de ejecutar lo anterior remplazamos los primeros 54 bytes de la nueva imagen por los de la original, hicimos esto para restablecer el header.

Resultado



AES Cipher Modes

CBC

Este modo de operacion requiere un vector de inicializacion por lo que la salida es distinta para la misma entrada y el mismo pass.

Sin embargo, es propenso a la propagacion de errores: una falla en un bloque altera a los siguientes. El proceso de descifrado puede paralelizarse, el de cifrado no.

Comando

```
openssl enc -aes-128-cbc -e -in secret.bmp -out CBCsecret.bmp -K 1001011 -iv 0010011
```

Donde:

Se usara AES de 128 bits con CBC como modo de operacion

La entrada es el archivo secret.bmp

La salida es el archivo CBCsecret.bmp

La llave es 1001011

Y el vector de inicializacion es 0010011

Resultado



Comparacion y conclusiones

```
chaos@chaos:~/Criptografia/tarea2$ cat Csecret.bmp | ent | head -n 2 ; cat CBCsecret.bmp | ent | head -n2
Entropy = 6.931572 bits per byte.
Entropy = 7.999819 bits per byte.
```

Vemos que el archivo generado usando CBC tiene un mayor indice de entropia.

El tamaño del archivo no se modifica.

El espacio de llaves es el mismo, sin embargo tienen ventajas y desventajas:

ECB

El cifrado es paralelizable

El error de bloque no es propagable

Menor carga para el procesador

No usa vector de inicializacion

Menor entropia

CBC

El cifrado no es paralelizable

Errores se propagan

Mayor carga

Uso de vector de inicializacion

Mayor entropia

Como vimos los modos de operacion tienen ventajas y desventajas, es importante conocerlas ya que siempre debemos escoger aquel que se ajuste mejor a las necesidades del desarrollo.

Referencia:

<https://notsoprogrammer.wordpress.com/2013/10/18/encrypting-pictures-aes-ecb-and-cbc/>