**Práctica DES: Modos de Operación**

|  |  |  |
| --- | --- | --- |
| Modo de operación | thundercats.bmp | paisaje.bmp |
| Original |  |  |
| ECB |  |  |
| CBC |  |  |
| CFB |  |  |
| OFB |  |  |

**Pruebas de Descifrado.**

**1. Descifrar cada imagen cifrada correctamente.**

Descifrado con el modo de operación **ECB** para thundercats\_ecb.bmp:

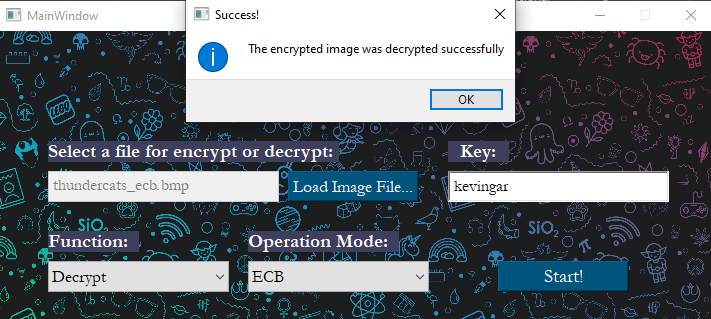


Imagen 1. Descifrado de thundercats\_ecb.bmp

El programa nos indica si la imagen pudo ser descifrada correctamente, en caso de que no haya ocurrido ningún error, el programa almacenará la imagen descifrada en el directorio **“decrypted-images”.**



Imagen 2. Imagen descifrada thundercats\_ecb.bmp

Descifrado con el modo de operación **ECB** para paisaje\_ecb.bmp:

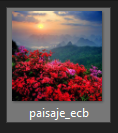
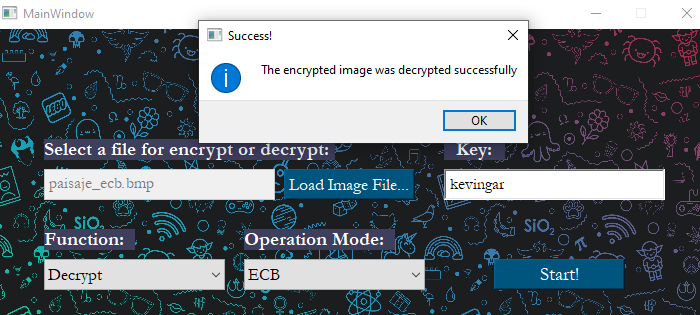


Imagen 3. Descifrado de paisaje\_ecb.bmp

Descifrado con el modo de operación **CBC** para thundercats\_cbc.bmp:

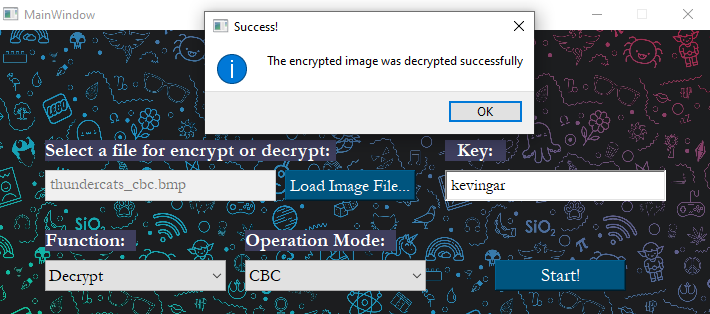


Imagen 4. Descifrado de thundercats\_cbc.bmp

Descifrado con el modo de operación **CBC** para paisaje\_cbc.bmp:

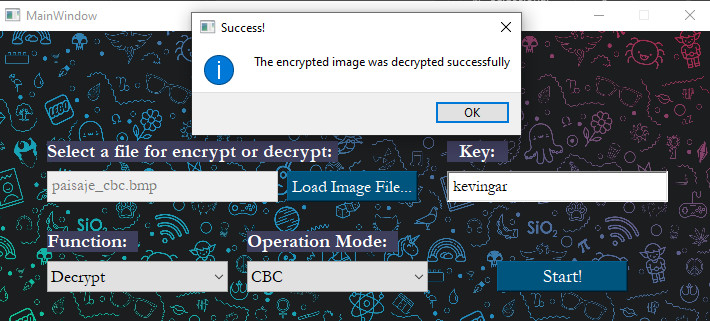
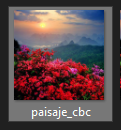


Imagen 5. Descifrado de paisaje\_cbc.bmp

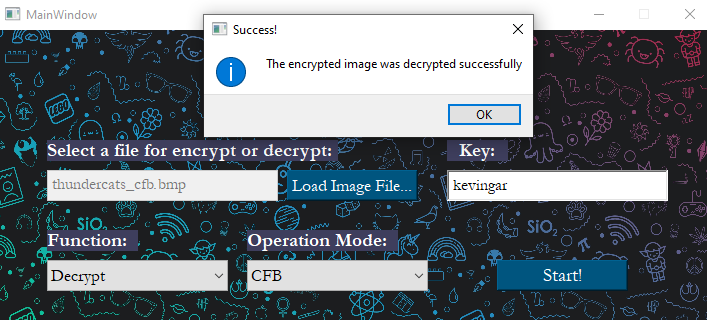
Descifrado con el modo de operación **CFB** para thundercats\_cfb.bmp:



Imagen 6. Descifrado de thundercats\_cfb.bmp

Descifrado con el modo de operación **CFB** para paisaje\_cfb.bmp:

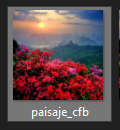
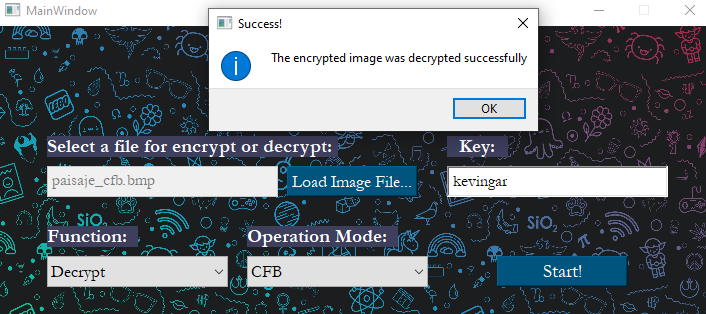


Imagen 7. Descifrado de paisaje\_cfb.bmp

Descifrado con el modo de operación **OFB** para thundercats\_ofb.bmp:

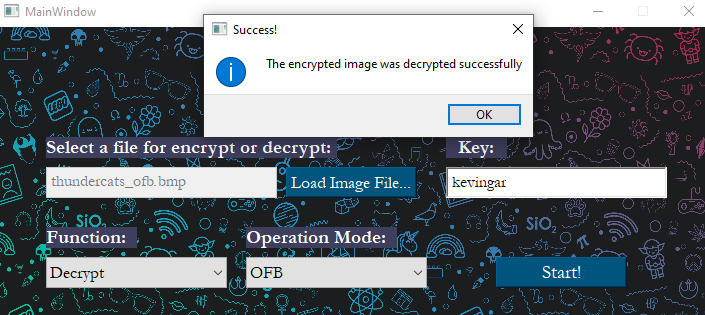


Imagen 8. Descifrado de thundercats\_ofb.bmp

Descifrado con el modo de operación **OFB** para paisaje\_ofb.bmp:

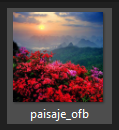
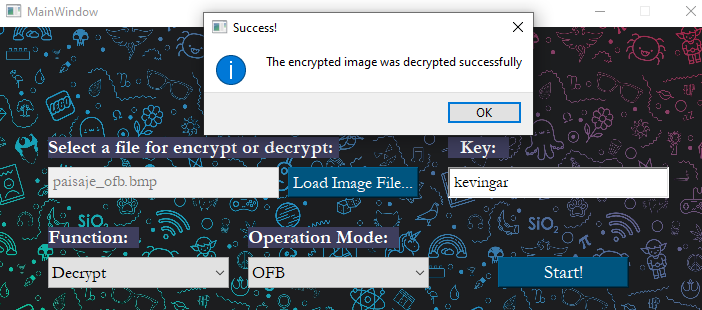


Imagen 9. Descifrado de paisaje\_ofb.bmp

**2. Descifrar \*\_CBC.bmp con el modo CFB**

Al descifrar **thundercats\_cbc.bmp** y **paisaje\_cbc.bmp** con el modo de operación CFB, el programa no marca ninguna excepción, debido a que ambos modos de operación mandan a la función de descifrado el mismo número de parámetros, pero lo único que cambia es el vector de inicialización con el que fue cifrada cada imagen, de tal modo que lo que obtenemos como resultado es:

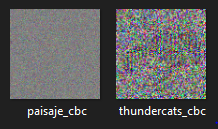


Imagen 10. Descifrado con un modo de operación incorrecto.

**3. Descifrar \*\_CFB.bmp con el modo ECB**

Al descifrar **thundercats\_cfb.bmp** y **paisaje\_cfb.bmp** con el modo de operación ECB, el programa arroja una excepción, ya que el modo de operación no requiere de **vector de inicialización**, así como tampoco necesita de un **padding**.

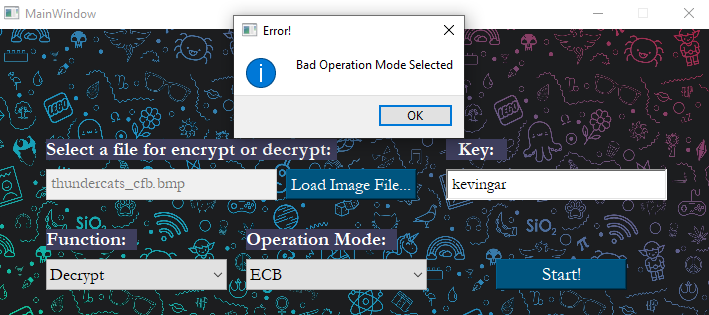


Imagen 11. Descifrado con un modo de operación incorrecto.

Así mismo el programa indica a que se debió el error en la salida por consola.



Imagen 12. Mensaje de error.

**4. Cifrar dos veces \*\_CFB.bmp con el modo OFB**

Cifrando dos veces **thundercats\_cfb.bmp** con OFB.

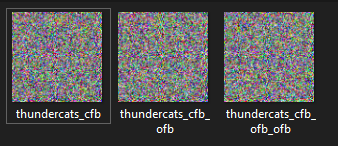


Imagen 12. Cifrando dos veces \*\_cfb con OFB.

Cifrando dos veces **paisaje\_cfb.bmp** con OFB.

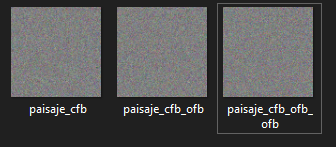


Imagen 13. Cifrando dos veces \*\_cfb con OFB.

**5. A la imagen cifrada \*\_ CBC dibujarle un cuadro y descifrar**

Se modifica la imagen **thundercats\_cbc.bmp** y **paisaje\_cbc.bmp** dibujando un cuadro negro, y se vuelve a descifrar.

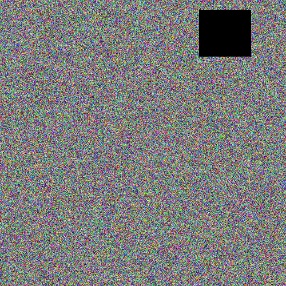
 

Imagen 14. thundercats\_cbc.bmp y paisaje\_cbc.bmp modificadas.

Al intentar descifrar ambas imágenes el programa arroja la siguiente excepción, esto se debe a que el **padding** inicial con el que fue cifrada la imagen cambio para un bloque, por lo que no es posible descifrar el archivo ya que el **padding** no corresponde con el que originalmente se utilizó.



Imagen 15. thundercats\_cbc.bmp y paisaje\_cbc.bmp excepción.

**6. A la imagen cifrada \*\_ CFB dibujarle un cuadro y descifrar.**

Se modifica la imagen **thundercats\_cbc.bmp** y **paisaje\_cbc.bmp** dibujando un cuadro negro, y se vuelve a descifrar.

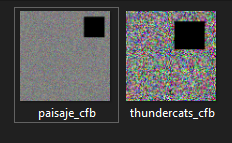


Imagen 14. thundercats\_cfb.bmp y paisaje\_cfb.bmp modificadas.

Finalmente, al intentar descifrar obtenemos el siguiente resultado:



Imagen 15. thundercats\_cfb.bmp y paisaje\_cfb.bmp descifradas.