TP3 Report

A85272	Jorge Mota
A83840	Maria Silva

This work has the objective to encrypt an image with both modes ECB and CBC and compare the visual result.

For that we created a python script to easily encrypt and decrypt images using these modes.

The file used for testing was a bmp image of a chess board pattern (`ex1.bmp`).


```
python3 image_encrypt.py
```

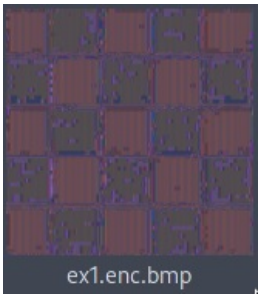
Encrypting this file results in an unreadable file because the bmp image metadata is also encrypted, so we execute the following command to visualize the content of it:

Note: The encrypted image will be stored in `ex1.enc.bmp` and the decrypted image will be stored in `ex1.dec.bmp` .

```
dd if=ex1.bmp of=ex1.enc.bmp bs=1 count=54 conv=notrunc
```

Using ECB

As we can see by the results the ECB encryption mode is not completly secure as we can check for patterns of the original image.



And the decryption was successful.

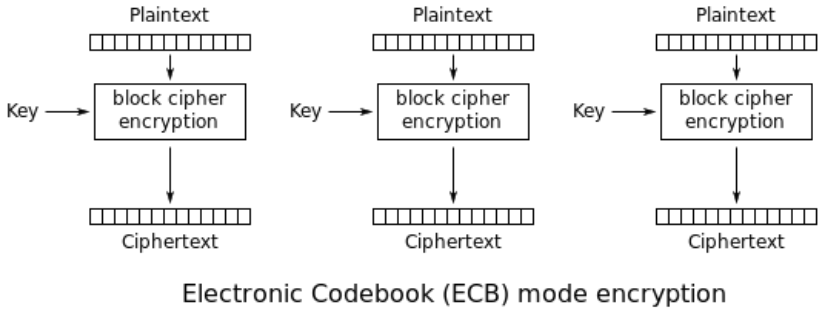
Using CBC

As we can see by the results the CBC encryption mode turns the encrypted image in a matrix of complete unreadable pixels.

And the decryption was successful.

Comparison

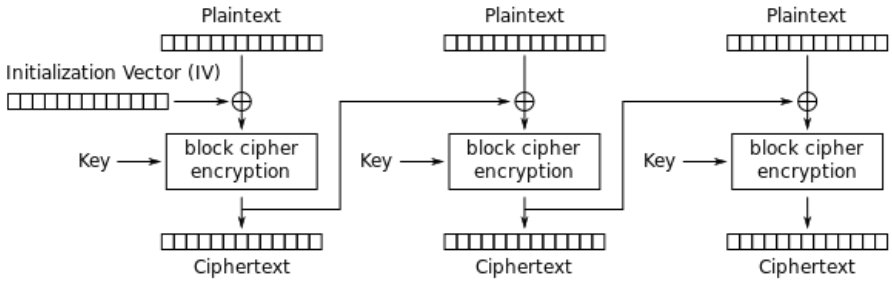
With knowledge of the process behind this two encryption modes, we could predict this results, since the ECB mode ciphers every block independently, with this we can predict that the encrypted result could present patters of the original data, and this can be very easily observed with images.



Electronic Codebook (ECB) mode encryption

On the other hand, the CBC mode uses the previous cipher block as the "initial vector" of the next iterations.

This being, the result will seem a lot more random than the previous mode.



Cipher Block Chaining (CBC) mode encryption