Name: Oscar Ashburn
ID: 1582735

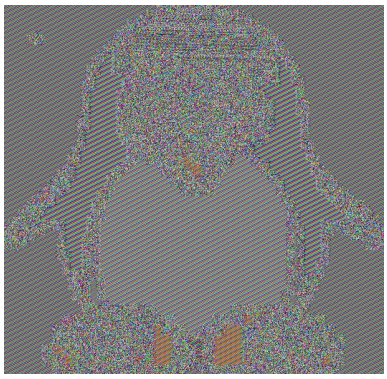
COMPX 518 Assignment 2

COMPX 518 Block Ciphers

Electronic Codebook Cipher (ECB)

The ECB(Electronic Codebook) block cipher mode functions by splitting the bytes of the image into blocks and encrypting each block with the same key. The result of the cipher is multiple cipher-texts joined together. This cipher requires data to be padded so that each block of ciphertext is the same size. This mode of AES encryption is ideal for small amounts of data as large amounts of data may assist an adversary in breaking the cipher.

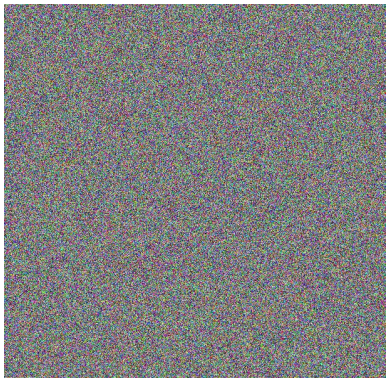
After encrypting the penguin image is still able to be seen and you can also still make out where the background of the image is after encrypting the bytes and converting them back to rgb. This is because the algorithm uses the same encryption key on each block of data.



Cipher Feedback (CFB)

The Cipher Feedback mode initially encrypts an initialization vector which is a pseudo random value with the key. A small number of bits is encrypted at a time (‘s’ bits)’.The leftmost ‘s’ bits of the iv are isolated and XORed with the segment of plaintext (segment size is = s).

The output of the image of the function produces a more seemingly random pattern of rgb values.



Cipher Block Chaining (CBC)

The Cipher Block Chaining mode uses the previously encrypted plaintext to XOR the next block of plaintext. Like CFB mode, CBC uses an initialization vector. CBC also needs to have padding as it works on fixed sized blocks.

The output again produces a seemingly random pattern of rgb values.