**Q .Write up for 2.2**: Can you derive any useful information about the original picture from the encrypted picture? Explain your observations for both the modes.

Answer :

ECB stands for the Electronic Codebook and CBC stands for Cipher Blocker Chaining which is an advance form of the black cipher encryption.

We can see in ECB on outline of the image is preserved in the encryption. While in the CBC image is not at all visible.

Below is the original image, ECB image and the CBC image.

**Below Original Image :**

Logo

Description automatically generated

**Below ECB Image :**

A picture containing text, clock

Description automatically generated

**Below CBC Image:**

Background pattern

Description automatically generated

**Q. 2.3 a. How much information can you recover by decrypting the corrupted file, if the encryption mode is ECB, CBC, or OFB, respectively? Please answer this question before you conduct this task, and then find out whether your answer is correct or wrong after**

**you finish this task.**

Answer

**Below is the ECB**

In this the message is divided into blocks, and each block is encrypted separately. So here in only a block is corrupted. Other block data is still visible.

Text

Description automatically generated

**Below is the CBC**

In this the plaintext of a block is combined with the ciphertext of the previous block is combined with ciphertext. Under this XOR of the plain text of one block with done with the encrypted output of the another block. The encryption is depended on the encrypted output of the previous one.

The output shows how one block is corrupted completed and one byte of next block is also corrupted because of this dependency.

Text

Description automatically generated

**Below is the OFB**

OFB is the output feedback mode which makes a block cipher into synchronous stream cipher, it generate keystream blocks , which are XORed with the plaintext blocks to get the ciphertext.

Under this corrupting a byte would result in corrupting only one byte in the original text after the decryption is done which we can see in the below output.

Text

Description automatically generated

**b. Explain why each algorithm reveals or doesn’t reveal information in the encrypted text?**

Answer

Under ECB some of the information is kind of reveal even in the encryption form. In the CBC data cannot be reveal the encryption is also dependent on the previous cipher text. In the OFB the encrypted text does not reveal anything since the keystream with initialization vector is difficult to make any patterns.

**c. What are the implications of these differences for Message Authentication Codes?**

**Would you use CBC or OFB? Explain your answer.**

Answer

Message authentication code is mechanism or service used to verify the integrity of a message. Under ECB the pattern can be easily found. Under CBC the change in the one clock will result in the changing of the next one also. Under OFC also uses the chaining mechanism still only the IV is updated and other part of the text remain the same. Because of these I would prefer to use **CBC**.