Report  
Exploring Symmetric Key Encryption Modes

# Task 1. Warm-up

1. Size of plaintext file (in bytes): 16 bytes
2. Size of above file after encryption (in bytes): 32 bytes
3. When you consider the file sizes that you recorded above, explain why the size of the ciphertext file is larger, and why the ciphertext file has that particular size.

The AES -128-cbc encryption mode use padding as it ensure the file size is 128 bit (16byte) or its multiply and when using iv it increased file size so padding is used to the next multiply which is 32 byte.

# Task 2. Encryption Modes

**ECB Mode**

1. When looking at the logo with the eye of a cryptanalyst, what repeated patterns do you see?

The encrypted logo using ECB mode shows noticeable patterns, it like the original image, due to ECB mode encrypting each block independently.

1. Size of the logo file (in bytes): 16782454
2. Size of logo file after encryption (in bytes): 16782454
3. Describe the encrypted logo.

XXXXXXX.

1. Referring to your observations in items 4 and 7, what is it about the inner-workings of ECB mode that caused it to do such a poor job of encrypting the logo.

ECB mode does a poor job of encrypting the logo because it encrypts identical plaintext blocks into identical ciphertext blocks, making patterns in the plaintext visible in the ciphertext.

**CBC Mode**

1. Size of logo file after encryption (in bytes): XXXXXX
2. Describe the encrypted logo.

Just a XXXXXX.

**CFB Mode**

1. Size of logo file after encryption (in bytes): XXXXXX
2. Describe the encrypted logo.

XXXXXXX.

**OFB Mode**

1. Size of logo file after encryption (in bytes): XXXXXX
2. Describe the encrypted logo.

XXXXXX.

1. Referring to your observations in items 10, 12 and 14, explain why these modes were able to do a better job of encrypting the logo.

Because CBC Mode& CFB and OFB mode uses an initialization vector (IV) and chains the encryption of each block with the previous block, making the encryption more secure and ensuring that identical plaintext blocks do not produce identical ciphertext blocks. .

1. The size of each encrypted logo was recorded in items 6, 9, 11, and 13. Explain why some of the file sizes are **larger** than the plaintext logo file (as recorded in item 5), and why some of them are the **same size** as the plaintext logo file.

Because XXXXXXXXXXXX.

1. Based on your simple observations, which of the encryption modes that you used in this assignment appear to provide semantic security? Why?

- Based on my observations, the encryption modes that provide semantic security are CBC, CFB, and OFB modes. These modes ensure that identical plaintext blocks do not result in identical ciphertext blocks by using an IV, thus preventing patterns from being visible in the ciphertext.