Report  
Exploring Symmetric Key Encryption Modes

# Task 1. Warm-up

1. Size of plaintext file (in bytes): XX bytes
2. Size of above file after encryption (in bytes): XX 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.

Because XXXXXXXXX.

# Task 2. Encryption Modes

**ECB Mode**

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

A XXXXXX.

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

XXXXXXXX.

**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 XXXXXXXX.

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?

XXXXXXXXXXXXXXXXXXXX.