Lab 2 Report  
Exploring Symmetric Key Encryption Modes

**Your Name Here**

# Task 1. Warm-up

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

TBD

# Task 2. Encryption Modes

**ECB Mode**

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

TBD

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

TBD

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.

TBD

**CBC Mode**

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

TBD

**CFB Mode**

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

TBD

**OFB Mode**

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

TBD

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.

TBD

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.

TBD

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

TBD

# Task 3. Error Propagation During Decryption

**Preparation**

|  |  |
| --- | --- |
| 1. Size of the file containing the Declaration of Independence: | \_\_\_\_\_\_\_\_\_\_ |
| 1. Number of AES blocks needed to encrypt the Declaration of Independence. Show your work. | \_\_\_\_\_\_\_\_\_\_ |
| 1. How many characters can AES encrypt in one block? (Hint: it takes one byte to encode a character). Show your work. | \_\_\_\_\_\_\_\_\_\_ |

**ECB Mode**

1. Describe the corruption that occurred when a ciphertext (with one-bit of corruption) was decrypted using ECB mode.

TBD

1. Referring to item 21, explain why ECB mode corrupted the plaintext in the manner you observed.

TBD

**CBC Mode**

1. Describe the corruption that occurred when a ciphertext (with one-bit of corruption) was decrypted using CBC mode.

TBD

1. Referring to item 23, explain why CBC mode corrupted the plaintext in the manner you observed.

TBD

# In Conclusion

1. Describe any extra experimentation you performed.

TBD (if any)

1. What did you learn from this exercise (if anything)? Please point out the observations or results that were surprising to you (if any). Also include those concepts that were made clearer (if any) by doing the assignment.

TBD (if any)

1. How could this exercise be improved?

TBD (if you see anything)