Matthew Austin

Network Security

Dr. Yang

October 2017

Lab 1

**3.2 Task 2: Encryption Mode - ECB vs. CBC**

2.) Yes, With ECB even though the file is covered in white noise, I am still able to see the image’s shape and outline. The encryption is not as strong as the CBC. With CBC, No I am not able to see the shape or outline of the image, it is successfully hidden and encrypted.

**3.3 Task 3: Encryption Mode - Corrupted Ciphertext**

1. If the encryption mode is ECB, I believe that you will be able to get more information. On the other hand with CBC, CFB, and especially OFB obtaining information from decryption will be more challenging.
2. Due to ECB being less effective at hiding the previous image information is more visible, so if the file is corrupted it will show more over CBC, CFB and especially OFB since they are more effective at hiding the previous image.
3. The implication of the differences were correct as stated above. An corrupted ECB file will provide more information when decrypted over a CBC, CFB, and OFB since a single bit error will propagate up to two blocks.

**3.4 Task 4: Padding**

2.) ECB and CBC have padding because the final block needs to be padded before encryption. CFB and OFB do not require padding since they work by XORing the plaintext with the output of the block.