SENG 360
Assignment #1

Jesse Browell
V00873161

1) Yes, using a different operating mode will result in a different in different ciphertext even with the same cipher. An operating mode decides how to use the cipher to create the ciphertext, so two different modes would result in two different processes being applied, creating different ciphertexts.

2) The difference I observed when comparing ECB and CBC was that with EBC it was possible to see parts of the unencrypted image in the encrypted image. This did not happen with CBC.

3) Yes, ECB and CBC use the same padding scheme. Both ECB and CBC require the size of the file to be divisible by the block size.

4) CBC and CFB do use different padding schemes because CFB does not require padding.

5) A single corrupted bit in ECB has a few characters in a row become corrupted, but the rest of the file is intact. CBC is similar to ECB but it is corrupted in two places. CFB has a large amount of text become corrupted but the text around it is intact. In OFB only a single character became corrupted.

6) For a single block, it is more secure to use ECB than CBC with a known IV. With CBC the encyryption of a block use the ciphertext of the block before it. In the case of a single block, this is not possible, making it less secure.

7) No, you can not change the key instead of the IV every time. If the only thing you change is the key when encrypting the same thing twice, the ciphertext will be similar. If you change the IV this is not a problem.

8) This attack can be prevented by using a different IV and key for encrypting the two different texts. The reason this attack works is because we can find the cipher for the file with a known plaintext and ciphertext. Also, the cipher is the same between the two files, allowing us to find the plaintext when we know the ciphertext.