Crypto Lab – Symmetric Key Ciphers

Kevin Nguyen

10/28/18

3.2 Task2 encryption mode

After performing the ECB encryption and the CBC encryption, it was easier to tell what the original image was of the ECB. But when I viwed the CBC image, it was impossible to see what the original image was. I think that the CBC is probably doing a lot better job of making encrypting the images that the ECB image.

3.3 task3 corrupted cipher text

After performing the corruption, a lot of the information is able to be translated back into a normal text. I feel like I can still gather a significant amount of text from the corrupted cipher text. I find that very interesting, with ECB I feel like it can be recovered relatively fine because of the way the block cipher is. I think that CBC will definitely be harder to decode because it relies on the previous information multiple times over. This means that one mistake, can cause an avalanche of corruption.

I think that the differences between the ciphers force people to think about what they want to do with their information. I think that the implication is that people should be using the strongest cipher.

Task 4

In my experimentation, ECB mode it seems that each block is very independent and is not affected by the padding

CBC only affects very few of the first blocks.

CFB the blocks are only affected the more blocks there are

Task 5

I was not able to finish this part substantially. I apologize for my lack of planning ahead.