Activity#3

DUE 17/11/2023 13.30

Implement a block cipher that encrypts a grayscale image at least 300x300 (four different shades of gray is ok) in a programming language of your choice.

Show that in EBC mode, we can guess the original image from the encrypted image by simply copying the original image and the encrypted image next to each other in your document.

Show that in CBC mode, we can NOT guess the original image from the encrypted image by simply copying the original image and the encrypted image next to each other in your document.

Add a README file that explains how to run your code and indicates the provided inputs and expected outputs.

Zip your source code, images, and .jar executable with the README file.

Math Students you can do either the coding or the assignment below:

Solve the problem #25, #31, #39, and #42 on Page 84 and 86 from the textbook.

25. Suppose that we use a block cipher to encrypt according to the rule

$$C_0 = \text{IV} \oplus E(P_0, K),\ C_1 = C_0 \oplus E(P_1, K),\ C_2 = C_1 \oplus E(P_2, K),\ \ldots$$

a. What is the corresponding decryption rule?

b. Give two security disadvantages of this mode as compared to CBC mode.

31. Suppose that Alice and Bob decide to always use the same IV instead of choosing IVs at random.

    a. Discuss a security problem this creates if CBC mode is used.

    b. Discuss a security problem this creates if CTR mode is used.

    c. If the same IV is always used, which is more secure, CBC or CTR mode?

39. Suppose Alice has four blocks of plaintext, P_0, P_1, P_2, P_3. She computes a MAC using key K_1, and then CBC encrypts the data using key K_2 to obtain C_0, C_1, C_2, C_3. Alice sends the IV, the ciphertext, and the MAC to Bob. Trudy intercepts the message and replaces C_1 with X so that Bob receives IV, C_0, X, C_2, C_3, and the MAC. Bob attempts to verify the integrity of the data by decrypting (using key K_2) and then computing a MAC (using key K_1) on the putative plaintext.

    a. Show that Bob will detect Trudy's tampering.

    b. Suppose that Alice and Bob only share a single symmetric key K. They agree to let $K_1 = K$ and $K_2 = K \oplus Y$, where Y is known to Alice, Bob, and Trudy. Assuming Alice and Bob use the same scheme as above, does this create any security problem?

42. Suppose that we define triple 3DES with a 168-bit key as

$$C = E(E(E(P, K_1), K_2), K_3).$$

    Suppose that we can compute and store a table of size 2^{56}, and a chosen plaintext attack is possible. Show that this triple 3DES is no more secure than the usual 3DES, which only uses a 112-bit key. Hint: Mimic the meet-in-the-middle attack on double DES.