UNIVERSITY AT ALBANY
State University of New York

DEPARTMENT OF COMPUTER SCIENCE

ICSI-426/526 Cryptography – Spring 2023

Homework 2

Give out date: February 16, 2023
Due date/time: March 9, 2023, 11:59 p.m. **Total marks: 13**

Late submissions would have penalty 5% every day up to five days.

Objective

The purpose of this homework is to solidify concepts of AES and its modes of operation, and image steganography.

Question 1 [7 Points]

You are required to implement the following modes of operation:

- Cipher Block Chaining (CBC)
- Output Feedback (OFB)

After implementation of the modes, you are required to encrypt text (as mentioned in the dataset below) and compute Index of Coincidence (IC) for each mode of operation, including Electronic Codebook (ECB).

Dataset: You will use a text file with the following characteristics –

i) Text length must be at least 2000 characters (main file).
ii) From the above original file, create two more sets of this file, in which the text is duplicated with approximately 25% and 50% ratio.

Report your observations and analysis for values of IC for each of the above three modes using each of the three text files. A table in the following format must be provided:

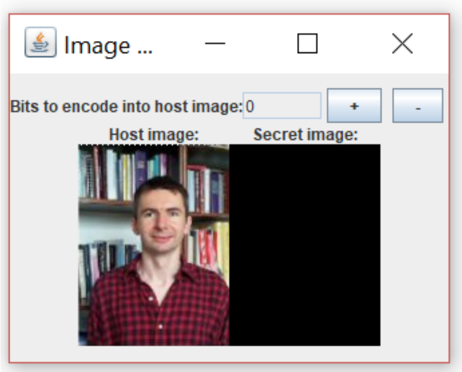
Mode	File with % duplication	IC
ECB	0	
	25	
	50	
CBC	0	
	25	
	50	
OFB	0	
	25	

	50	

You may use any publicly available AES code or the AES code provided at. Provide the details of the source of the AES code that you use. Note that the implementation of the modes should be your own.

Question 2 [6 Points]

Consider the image hiding example shown in the figure below:



Bits to encode into host image: 0

The java class **ImageHiding.java** (provided) contains code to hide one image (Secret Image *S*) in another (Host Image *H*) – images also provided. The embedding operation (original) is as follows: Hide MSB of S in LSB of H, and Red of S going to Red of H, Green of S to Green of H, Blue of S to Blue of H.

You are required to extend the application to perform the following operations:

- Hide MSB of S in MSB of H.
- Hide LSB of S in LSB of H.
- Hide LSB of S in MSB of H.

You also need to make appropriate changes to the GUI to give the user an option to select one of the four data hiding operations mentioned above. Implement these operations and report your observations for all three data hiding operations compared to the original operation.

Submission Instructions

You must submit the following via UAlbany Blackboard:

(a) Source code along with the instructions to run it.
(b) A pdf file containing your code for Questions 1 and 2.
(c) A pdf file containing answers to Questions 1 and 2.
(d) A video (of max 5 minutes) with voiceover that shows the working of your program.