

## **Lab 1**

This lab is divided into 4 sections namely:

1. LFSR
2. LFSR Sum
3. Block Cipher
4. Cryptography with images (AES modes)

Jupyter notebook is provided to you to run all the cells and show the output of each cell. Besides this, the following questions require your answer in the notebook.

Question on LFSR

#2.

Question on LFSR Sum

#5.

Question on Block Cipher

#8.

Question on cryptography with images

#19. Besides running the cell, send secret\_image2 as your submission.

Question on AES

#31. Besides running the cell, submit the e\_secret\_image2\_ecb and d\_secret\_image2\_ecb

Question on AED

#32. Besides running the cell, submit the e\_secret\_image2\_cbc and d\_secret\_image2\_cbc

### **What to Submit:**

1. Jupyter file with your name
2. Images

### **Rubric:**

Task	Points
2	15
5	15
8	20
19	15
31	20
32	15

**Optional: Extra credit**