Assignment 2

1. What is the difference between block and stream cipher ? 5
2. What is the difference between diffusion and confusion ? 5
3. What are the parameters that define a simple Feistel cipher ? 5
4. Explain the avalanche effect in a crypto system. 5
5. Explain each step in a single round of DES algorithm implementation. 5
6. Why is DES considered less secure nowadays ? 5
7. Using the S-Box given below, explain what the output would be if the input is $(ABC8E2193ACD)_{16}$. Given that in a sequence of 6 bits, the middle 4 bits represent column number and extreme two bits represent row number. 10

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

8. Why is the AES algorithm considered better than the DES ? 5
9. What is the difference between groups, rings and fields ? 5
10. Using the concept of $GF(2^4)$, write down the polynomial equations, derived from binary representations 0000 to 1111. 10
11. Based on $GF(2^4)$ what is the solution on adding $(C)_{16}$ and $(8)_{16}$? 5
12. What would be the output from the Shift Rows layer in AES if the input provided is $(ABC8E219\ 3ACD9F25\ 7634A21C\ 2A5B45FE)_{16}$ 10
13. In this question you will learn how to apply concept of steganography. Follow the instructions as provided below to hide messages in images. You will have to answer part v and provide three screenshots showing how you implemented the steps. 10
    a. Use your web browser and using your favorite search engine search for "**OpenPuff**".
    b. Click on the **Source Page** and then click **Manual** to open the OpenPuff manual. Save this file to your computer. Read through the manual to see the different features available.
    c. Click your browser's back button to return to the home page
    d. Click OpenPuff to download the program.
    e. Navigate to the location of the download and uncompress (unzip) the Zip file on your computer.
    f. Now create a carrier file that will contain the hidden message. Open a Windows search box and enter Snipping Tool.
    g. Launch Snipping Tool
    h. Click the New menu arrow, then click Window Snip.
    i. Capture the image of one of the pages of the OpenPuff manual. Click File and Save As. Enter **Carrier1.png** and save to a location such as the desktop
    j. Now create the secret message to be hidden. Create a new Word file and enter: **This is a secret message.**

k. Save this file as **Message.docx**
l. Exit Word.
m. Create a Zip file from **Message**. Navigate to the location of this file through Windows Explorer and click the right mouse button.
n. Click **Send to** and select **Compressed (zipped) folder** to create the Zip file.
o. Navigate to the OpenPuff directory and double-click **OpenPuff.exe**
p. Click **Hide** in the **Steganography section.**
q. Under (1), create three unrelated passwords and enter them into **Cryptography (A), (B), and (C).**
r. Under (2), locate the message to be hidden. Click **Browse** and navigate to the file **Message.zip**. Click **Open.**
s. Under (3), select the carrier file. Click **Add** and navigate to **Carrier1.png** and click **Open**.
t. Click **Hide Date!**
u. Navigate to a different location than that of the carrier files and click **OK**. Click **Done** in the **Task Report** window.
v. After the processing is completed, navigate to the location of the carrier file that contains the message and open the file. Can you detect anything different with the file now that it contains the message?
w. Now uncover the message. Close the OpenPuff Data Hiding screen to return to the main menu.
x. Click **Unhide.**
y. Enter the three passwords.
z. Click **Add Carriers** and navigate to the location of **Carrier1** that contains the hidden message and click **Open.**
aa. Click **Unhide** and navigate to a location to deposit the hidden message. When it has finished processing click **OK**
bb. Click **Done** after reading the report.
cc. Go to that location and you will see **Message.zip**
dd. Take a screen shot of the OpenPuff window and paste it in your word document that you will submit.
ee. Close OpenPuff and close all windows.

14. The chart for Vignere Cipher is available in the slides on blackboard under Week 3. Use the chart to answer Q14 and Q15. Use Vignere Cipher to encode the text NETWORKSECURITY. 5

15. With the starting position K = 7, S = 3, show the cipher text for the following text 10
LORENZCIPHER