Assignment – 1

CS3801 – Computer Security

The objective of this assignment is to assess the student knowledge and skill against the learning outcome "**Encrypt decrypt texts using a variety of classical and modern ciphers**" giving hands-on exercises to apply classical symmetric encryption techniques **(5 Points)**

Apply symmetric encryption technique and find the following cipher. For this task take **your full name (first, middle and last) as the plain message**

a. Playfair cipher with **Sydney as key** **(2 Points)**
To apply the Playfair cipher, we need to construct a 5x5 key matrix based on the given key "Sydney". Here are the steps:

Step 1: Construct the Playfair matrix based on the key "Sydney":
S Y D N E
A B C F G
H I K L M
O P Q R T
U V W X Z

Step 2: Prepare the plaintext by dividing it into pairs of letters, adding a filler if needed:
Plaintext: HA YA SA LI MA LD OS AR IX

Step 3: Apply the Playfair cipher rules to each pair of letters in the plaintext:

Pair: HA
- H maps to "SY" in the Playfair matrix.
- A maps to "DY" in the Playfair matrix.

Pair: YA
- Y maps to "DY" in the Playfair matrix.
- A maps to "SY" in the Playfair matrix.

Pair: SA
- S maps to "LG" in the Playfair matrix.
- A maps to "SY" in the Playfair matrix.

Pair: LI
- L maps to "IM" in the Playfair matrix.
- I maps to "LI" in the Playfair matrix.

Pair: MA
- M maps to "AL" in the Playfair matrix.
- A maps to "SY" in the Playfair matrix.

Pair: LD
- L maps to "IM" in the Playfair matrix.
- D maps to "SY" in the Playfair matrix.

Pair: OS
- O maps to "LG" in the Playfair matrix.
- S maps to "LG" in the Playfair matrix.

Pair: AR
- A maps to "SY" in the Playfair matrix.
- R maps to "IM" in the Playfair matrix.

Pair: IX
- I maps to "LI" in the Playfair matrix.
- X maps to "IM" in the Playfair matrix.

Step 4: Combine the ciphertext obtained from each pair:

Ciphertext: SY DY DY SY LG SY IM LI AL SY IM SY LG IM LI

b. Rail fence cipher with depth 2 **(1 Points)**

The Rail Fence cipher rearranges the plaintext by writing it in a zigzag pattern along a set number of "rails" or lines. In this case, we use a depth of 2.

To encrypt the plaintext "Haya Salim Al-Dosari" using the Rail Fence cipher with depth 2, we write the letters in a zigzag pattern as follows:

H A Y A S A L I M A L D O S A R I
\ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ /
A Y S L M L O S R I H A D A A I

The encrypted ciphertext is obtained by reading the letters row by row from the zigzag pattern:

AYSLMLOSRIHADAAI

c. Vigenère cipher with **Sydney as key** **(2 Points)**

To encrypt the plaintext "Haya Salim Al-Dosari" using the Vigenère cipher with the key "Sydney," we repeat the key to match the length of the plaintext:

Key: S Y D N E Y S Y D N E Y S Y D N E Y S Y D N E Y S Y D N E Y
Plaintext: H A Y A S A L I M A L - D O S A R I

To encrypt each letter, we find the corresponding shift value determined by the key:

H + S = T
A + Y = X
Y + D = H
A + N = O
S + E = X
A + Y = Y
L + S = Q
I + Y = O
M + D = Q
A + N = O
L + E = T
Y = -
D + S = G
O + Y = Z
S + D = W
A + N = O
R + E = U
I + Y = J

The encrypted ciphertext is: " TXHOXYQOQOTYGZWOUJ".