Name: Muhammad Rafiq

Seat No: B17101061

Course: Network Security & Cryptography (NS'21 Lab)

Assignment : Assignment # 5

Section: A

In [131]:

```
import numpy as np
class Hill_Cipher:

    def __find_a_inverse(self, a):
        a_list = [1,3,5,7,9,11,15,17,19,21,23,25]
        for i in a_list:
            if modulo((i*a), 26) == 1:
                return i

    def hill_decrypt(self, message, key):
        print("The Message To be Decrypted: ")
        print(message)
        det = np.linalg.det(key)
        key = [[key[1][1], -key[0][1]], [-key[1][0], key[0][0]]]
        key = np.array(key,dtype = 'int')
        det = int(det)
        if det < 0:
            det = 26 +  det
        det = find_a_inverse(det)
        key = (det * key)  % 26
        arr = np.array(list(message)) if len(message) %2 == 0 else np.array(
        final_ans = ""
        for i in range(0,len(arr)-1,2):
            ans = np.dot(key, np.array([ord(arr[i])-65, ord(arr[i+1])-65]))
            ans = ans % 26
            final_ans += chr(ans[0]+65) + chr(ans[1] + 65)
        print("\n\n")
        print("The Plain Text is: ")
        print(final_ans)

    def hill_encrypt(self, message, key):
        message = message.upper().replace(" ","")
        print("The Message To be Encrypted: ")
        print(message)
        key = np.array(key)
        key = key % 26
        key = np.where(key > 0 , key, 26 - key)
        arr = np.array(list(message)) if len(message) %2 == 0 else np.array(
        final_ans = str()
        for i in range(0,len(arr)-1,2):
            ans = np.dot(key, np.array([ord(arr[i])-65, ord(arr[i+1])-65]))
            #print(key, "\t",[arr[i], arr[i + 1]],"\t", [ord(arr[i])-65, ord
                    #,"\t",ans %26,"\t",chr(ans[0]%26+ 65) + chr(ans[1]%26 +
            ans = ans % 26
            final_ans += chr(ans[0]+ 65) + chr(ans[1] + 65)
        print("\n\n")
        print("The Cipher Text is: ")
        print(final_ans)

```

1- Encrypt the message "either you value the things or you lost value" using Hill cipher

Key= [18 9]

[27 36]

In [132]:
```
hill = Hill_Cipher()
```

In [133]:
```
hill.hill_encrypt("either you value the things or you lost value", [[18,9],[
```

```
The Message To be Encrypted:
EITHERYOUVALUETHETHINGSORYOULOSTVALUE


The Cipher Text is:
OGPLRSMIDWVGGIPLJMQJCVICCXQGMVBAOVODTA
```

2-Decrypt the message "APADJTFWLFJ"

Key= [7 8] ¶

[11 11]

In [134]:
```
hill.hill_decrypt("APADJTFWLFJ",[[7,8],[11,11]])
```

```
The Message To be Decrypted:
APADJTFWLFJ


The Plain Text is:
SHORTELRVWDS
```

M. Rafiq
B17101061

Hill Cipher

Encrypt the message "either you value the things or you lost value"

$$Key = \begin{bmatrix} 18 & 9 \\ 27 & 36 \end{bmatrix}$$

$$C = KA \bmod 26.$$

Now for Key

$$Key = \begin{bmatrix} 18 & 9 \\ 27 & 36 \end{bmatrix} \bmod 26$$

$$Key = \begin{bmatrix} 18 & 9 \\ 1 & 10 \end{bmatrix}.$$

Now, for C

K A Avalue C

$$\begin{bmatrix} 18 & 9 \\ 1 & 10 \end{bmatrix} * \begin{bmatrix} E \\ I \end{bmatrix} * \begin{bmatrix} 4 \\ 8 \end{bmatrix} = \begin{bmatrix} 144 \\ 84 \end{bmatrix} = \begin{bmatrix} 14 \\ 6 \end{bmatrix} = \begin{bmatrix} O \\ G \end{bmatrix}$$

$$\begin{bmatrix} 18 & 9 \\ 1 & 10 \end{bmatrix} * \begin{bmatrix} T \\ H \end{bmatrix} * \begin{bmatrix} 19 \\ 7 \end{bmatrix} = \begin{bmatrix} 405 \\ 89 \end{bmatrix} = \begin{bmatrix} 15 \\ 11 \end{bmatrix} = \begin{bmatrix} P \\ L \end{bmatrix}$$

$$\begin{bmatrix} 18 & 9 \\ 1 & 10 \end{bmatrix} * \begin{bmatrix} E \\ R \end{bmatrix} * \begin{bmatrix} 4 \\ 17 \end{bmatrix} = \begin{bmatrix} 225 \\ 174 \end{bmatrix} = \begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} R \\ S \end{bmatrix}$$

K A Av C

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}4\\ 0\end{bmatrix} \times \begin{bmatrix}24\\ 14\end{bmatrix} = \begin{bmatrix}558\\ 164\end{bmatrix} = \begin{bmatrix}12\\ 8\end{bmatrix} = \begin{bmatrix}M\\ I\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}4\\ V\end{bmatrix} \times \begin{bmatrix}20\\ 21\end{bmatrix} = \begin{bmatrix}549\\ 230\end{bmatrix} = \begin{bmatrix}3\\ 22\end{bmatrix} = \begin{bmatrix}D\\ W\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}A\\ L\end{bmatrix} \times \begin{bmatrix}0\\ 4\end{bmatrix} = \begin{bmatrix}99\\ 110\end{bmatrix} = \begin{bmatrix}21\\ 6\end{bmatrix} = \begin{bmatrix}V\\ G\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}4\\ E\end{bmatrix} \times \begin{bmatrix}20\\ 4\end{bmatrix} = \begin{bmatrix}396\\ 60\end{bmatrix} = \begin{bmatrix}6\\ 8\end{bmatrix} = \begin{bmatrix}G\\ I\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}I\\ H\end{bmatrix} \times \begin{bmatrix}19\\ 7\end{bmatrix} = \begin{bmatrix}405\\ 84\end{bmatrix} = \begin{bmatrix}15\\ 11\end{bmatrix} = \begin{bmatrix}P\\ L\end{bmatrix}.$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}6\\ T\end{bmatrix} \times \begin{bmatrix}4\\ 19\end{bmatrix} = \begin{bmatrix}243\\ 194\end{bmatrix} = \begin{bmatrix}9\\ 12\end{bmatrix} = \begin{bmatrix}I\\ m\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}H\\ I\end{bmatrix} \times \begin{bmatrix}7\\ 8\end{bmatrix} = \begin{bmatrix}198\\ 87\end{bmatrix} = \begin{bmatrix}16\\ 9\end{bmatrix} = \begin{bmatrix}P\\ J\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}N\\ G\end{bmatrix} \times \begin{bmatrix}13\\ 6\end{bmatrix} = \begin{bmatrix}288\\ 77\end{bmatrix} = \begin{bmatrix}2\\ 21\end{bmatrix} = \begin{bmatrix}C\\ V\end{bmatrix}$$

M-Rafiq
B17C0061

K A Dv C

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}5\\ 0\end{bmatrix} \times \begin{bmatrix}18\\ 14\end{bmatrix} = \begin{bmatrix}450\\ 158\end{bmatrix} = \begin{bmatrix}8\\ 2\end{bmatrix} = \begin{bmatrix}I\\ C\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}R\\ Y\end{bmatrix} \times \begin{bmatrix}17\\ 24\end{bmatrix} = \begin{bmatrix}522\\ 257\end{bmatrix} = \begin{bmatrix}2\\ 27\end{bmatrix} = \begin{bmatrix}C\\ X\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}0\\ 4\end{bmatrix} \times \begin{bmatrix}14\\ 20\end{bmatrix} = \begin{bmatrix}432\\ 214\end{bmatrix} = \begin{bmatrix}16\\ 6\end{bmatrix} = \begin{bmatrix}O\\ G\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}L\\ 0\end{bmatrix} \times \begin{bmatrix}11\\ 14\end{bmatrix} = \begin{bmatrix}324\\ 151\end{bmatrix} = \begin{bmatrix}12\\ 21\end{bmatrix} = \begin{bmatrix}M\\ V\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}S\\ T\end{bmatrix} \times \begin{bmatrix}18\\ 19\end{bmatrix} = \begin{bmatrix}495\\ 208\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix} = \begin{bmatrix}B\\ A\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}V\\ A\end{bmatrix} \times \begin{bmatrix}21\\ 0\end{bmatrix} = \begin{bmatrix}378\\ 21\end{bmatrix} = \begin{bmatrix}14\\ 21\end{bmatrix} = \begin{bmatrix}O\\ V\end{bmatrix}$$

$$\begin{bmatrix}18 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}L\\ 4\end{bmatrix} \times \begin{bmatrix}4\\ 20\end{bmatrix} = \begin{bmatrix}378\\ 216\end{bmatrix} = \begin{bmatrix}14\\ 3\end{bmatrix} = \begin{bmatrix}O\\ D\end{bmatrix}$$

$$\begin{bmatrix}12 & 9\\ 1 & 10\end{bmatrix} \times \begin{bmatrix}E\\ X\end{bmatrix} \times \begin{bmatrix}7\\ 23\end{bmatrix} = \begin{bmatrix}279\\ 234\end{bmatrix} = \begin{bmatrix}17\\ 0\end{bmatrix} = \begin{bmatrix}R\\ A\end{bmatrix}$$

Encrypted text would be

OCGPLRSMIDWVGGIPLJMOJCVI
CCXOGMYBAOYODIA

Q Decrypt the message "APADJTFWLFJ"

$$Key = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

Formula, $P = K^{-1} A \bmod 26$

Finding K^{-1}

$$K^{-1} = \frac{1}{-11} \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

$$K^{-1} = \frac{1}{15} \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

$$K^{-1} = 7 \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 77 & -56 \\ -77 & 49 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix}$$

K^{-1} A P

$$\begin{bmatrix} 25 & 22 \\ 1 & 27 \end{bmatrix} \times \begin{bmatrix} A \\ P \end{bmatrix} \times \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 370 \\ 345 \end{bmatrix} = \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} S \\ H \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \times \begin{bmatrix} A \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 66 \\ 69 \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 0 \\ E \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \times \begin{bmatrix} J \\ T \end{bmatrix} \times \begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} T \\ E \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \times \begin{bmatrix} F \\ W \end{bmatrix} \times \begin{bmatrix} 5 \\ 22 \end{bmatrix} \times \begin{bmatrix} 11 \\ 17 \end{bmatrix} = \begin{bmatrix} L \\ R \end{bmatrix}$$

$$\begin{bmatrix} 25 & 22 \\ 1 & 23 \end{bmatrix} \times \begin{bmatrix} L \\ F \end{bmatrix} \times \begin{bmatrix} 11 \\ 5 \end{bmatrix} = \begin{bmatrix} 21 \\ 22 \end{bmatrix} = \begin{bmatrix} V \\ W \end{bmatrix}$$

$$\begin{bmatrix} 21 & 22 \\ 1 & 23 \end{bmatrix} \times \begin{bmatrix} 3 \\ 21 \end{bmatrix} \times \begin{bmatrix} 9 \\ 23 \end{bmatrix} = \begin{bmatrix} 7 \\ 12 \end{bmatrix} = \begin{bmatrix} D \\ S \end{bmatrix}$$

Now, decrypted message is

SHORTFLRWDS.