Ministry of Higher Education And Scientific Research

AL-Mustaqbal University College

Department of Computer Engineering Techniques

Experiment 7

Encrypt by using Hill cipher

Eng:- Shaymaa Fakhir AL-Hamdany

$C = KP \bmod 26$

For **example**, we will illustrate the cipher with n=2. Consider the following key:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}$$

To encrypt a plaintext, group the plaintext in pairs: "**math**", for **example**. Convert each letter to its numerical equivalent, mod 26, and write it in a nx1 matrix as follows:

$\begin{pmatrix} 12 \\ 0 \end{pmatrix}$ stands for "**ma**"

Now, multiply the encryption key by the plaintext and reduce mod 26 to get the ciphertext:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} 36 \\ 72 \end{pmatrix} \bmod 26 = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$$, which corresponds to the ciphertext **KU**.

Here is the encryption of "**th**":

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 64 \\ 149 \end{pmatrix} \bmod 26 = \begin{pmatrix} 12 \\ 19 \end{pmatrix}$$, which corresponds to the ciphertext **MT**.

Ciphertext: **KUMT**

Encrypt Hill Cipher:

```
clc;
clear all;
close all;

k=[3 1;6 5];
p=input('enter plaintext: ','s');
p=lower(p);
lp=length(p);
z=mod(lp,2);
if z ~= 0;
   e=2-z;
   for i=1:e
       p(lp+i)='x';
   end
end
for i=1:2:lp
    s=double(p(i:i+1))'-97;
    c(i:i+1)=mod(k*s,26);
end
c=char(c+65);
disp(['The ciphertext : ' c])
```

enter plaintext: math

The ciphertext : KUMT