The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 4

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective :

- **Encryption and Decryption using Hill Cipher when 2D Key.**

Hill Cipher

This encryption algorithm takes m successive plaintext letters and substitutes for them m Ciphertext letters. The Hill cipher uses matrix multiplication, mod 26. In particular, the encryption key is an $n * n$ matrix, where n is the block size. System can be described as follows:

Encryption equation will be : $C = (P * K) \ mod \ 26$

Decryption equation will be : $P = (C * K^{-1}) \ mod \ 26$

Where P → Plaintext

C → Ciphertext

K → Key

Note: The Key must be in the form of a matrix.

Hill Cipher

Alice

Sender

Bob

Receiver

$$C = (P * K)\ mod\ 26$$

K

Matrix

Encryption

K^{-1}

Inverse Matrix

$$P = (C * K^{-1})\ mod\ 26$$

Decryption

Cipher text

Example 1

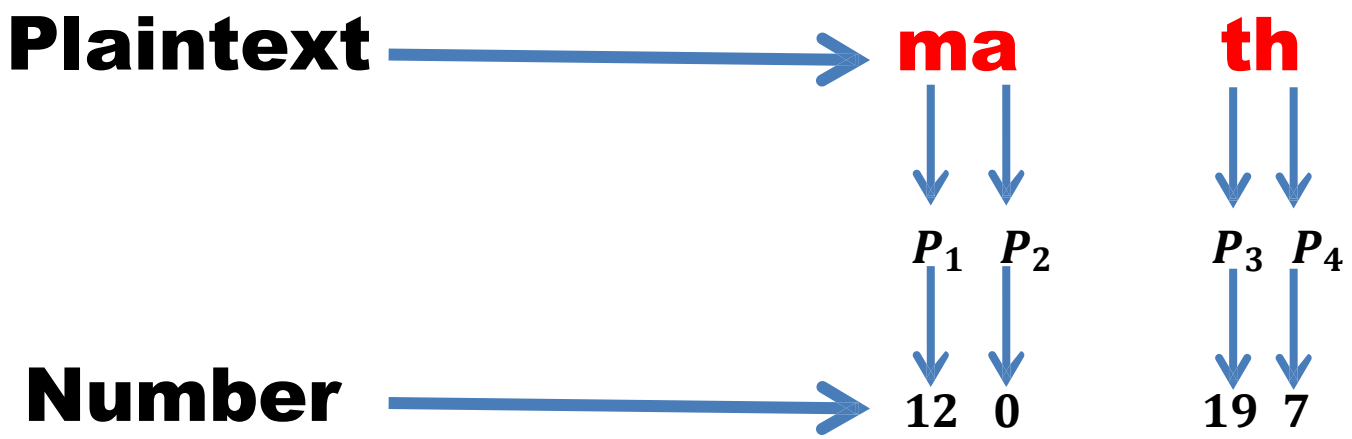
Encrypt and decrypt the Plaintext "math" by using Hill Cipher with the Key:

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

Ans:-

1. Encryption Algorithm

$$C = (P * K) \, mod \, 26$$



$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \left(\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod \, 26$$

$$\begin{pmatrix} \boldsymbol{C_1} \\ \boldsymbol{C_2} \end{pmatrix} = \left(\begin{pmatrix} m \\ a \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod\ 26$$

$$\begin{pmatrix} \boldsymbol{C_1} \\ \boldsymbol{C_2} \end{pmatrix} = \left(\begin{pmatrix} 12 \\ 0 \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod\ 26$$

$C_1 = ((12 * 3) + (0 * 1)) \bmod 26$

$C_1 = (36) \bmod 26$

$C_1 = 10 = \mathrm{K}$

$C_2 = ((12 * 6) + (0 * 5)) \bmod 26$

$C_2 = (72) \bmod 26$

$C_2 = 20 = \mathrm{U}$

$\mathbf{P_3 = t = 19}$

$\mathbf{P_4 = h = 7}$

$$\begin{pmatrix} \boldsymbol{C_3} \\ \boldsymbol{C_4} \end{pmatrix} = \left(\begin{pmatrix} P_3 \\ P_4 \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod\ 26$$

$$\begin{pmatrix} C_3 \\ C_4 \end{pmatrix} = \left(\begin{pmatrix} t \\ h \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod\ 26$$

$$\begin{pmatrix} C_3 \\ C_4 \end{pmatrix} = \left(\begin{pmatrix} 19 \\ 7 \end{pmatrix} * \begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix} \right) mod\ 26$$

$$C_3 = \big((19 * 3) + (7 * 1)\big) \bmod 26$$
$$C_3 = (64) \bmod 26$$
$$C_3 = 12 = M$$

$$C_4 = \big((19 * 6) + (7 * 5)\big) \bmod 26$$
$$C_4 = (149) \bmod 26$$
$$C_4 = 19 = T$$

The Ciphertext is : $C_1C_2C_3C_4$ → **"KUMT"**

Inverse of the Matrix

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

$$\mathbf{K^{-1}} = \left(\left(\mathbf{det(K)} \right)^{-1} * \mathbf{K^{T}} \right) \mathbf{mod\ 26}$$

$$det(K) = \left((3 * 5) - (1 * 6)\right) mod\ 26$$

$$det(K) = \left((15) - (6)\right) mod\ 26$$

$$det(K) = (9)\ mod\ 26 = 9$$

$$\left(det(K)\right)^{-1} = 3$$

$$K^{T} = \begin{pmatrix} 5 & -1 \\ -6 & 3 \end{pmatrix}$$

$$K^{-1} = \left((3) * \begin{pmatrix} 5 & -1 \\ -6 & 3 \end{pmatrix} \right) mod\ 26$$

$$K^{-1} = \begin{pmatrix} 3 * 5 & 3 * (-1) \\ 3 * (-6) & 3 * 3 \end{pmatrix} mod\ 26$$

$$K^{-1} = \begin{pmatrix} 15 & -3 \\ -18 & 9 \end{pmatrix} mod\ 26$$

$$K^{-1} = \begin{pmatrix} 15\ mod\ 26 & -3\ mod\ 26 \\ -18\ mod\ 26 & 9\ mod\ 26 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}$$

Verify

We can also verify this by multiplying both matrices in question together:

$$\left(\boldsymbol{K} * \boldsymbol{K^{-1}}\right) \boldsymbol{mod}\ \mathbf{26} = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}$$

$$\left(\begin{pmatrix} \mathbf{3} & \mathbf{1} \\ \mathbf{6} & \mathbf{5} \end{pmatrix} * \begin{pmatrix} \mathbf{15} & \mathbf{23} \\ \mathbf{8} & \mathbf{9} \end{pmatrix}\right) \boldsymbol{mod}\ \mathbf{26}$$

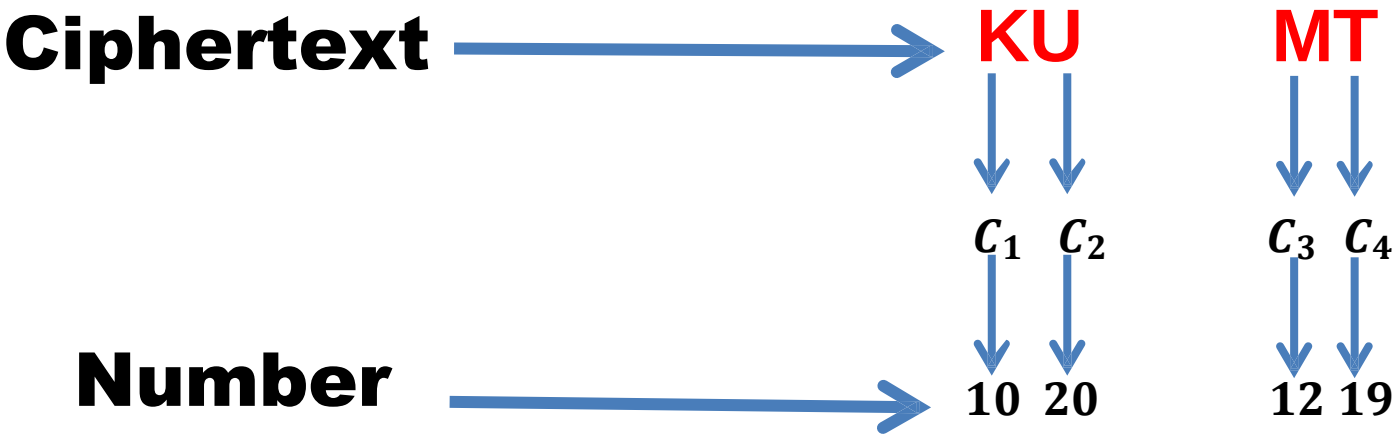
$$\begin{pmatrix} (3 * 15) + (1 * 8) & (3 * 23) + (1 * 9) \\ (6 * 15) + (5 * 8) & (6 * 23) + (5 * 9) \end{pmatrix} mod\ 26$$

$$\begin{pmatrix} 53 & 78 \\ 130 & 183 \end{pmatrix} mod\ 26$$

$$\begin{pmatrix} 53\ mod\ 26 & 78\ mod\ 26 \\ 130\ mod\ 26 & 183\ mod\ 26 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2. Decryption Algorithm

$$P = (C * K^{-1}) \; mod \; 26$$



$C_1 = K = 10$
$C_2 = U = 20$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \left(\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod \; 26$$

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \left(\begin{pmatrix} K \\ U \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod \; 26$$

$$\begin{pmatrix} \boldsymbol{P_1} \\ \boldsymbol{P_2} \end{pmatrix} = \left(\begin{pmatrix} 10 \\ 20 \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod\ 26$$

$P_1 = \big((10 * 15) + (20 * 23)\big)\ mod\ 26$

$P_1 = \big((150) + (460)\big) \bmod 26$

$P_1 = (610) \bmod 26 = 12 = \mathrm{m}$

$P_2 = \big((10 * 8) + (20 * 9)\big) \bmod 26$

$P_2 = \big((80) + (180)\big) \bmod 26$

$P_2 = (260) \bmod 26 = 0 = \mathrm{a}$

$\boldsymbol{C_3 = M = 12}$

$\boldsymbol{C_4 = T = 19}$

$$\begin{pmatrix} \boldsymbol{P_3} \\ \boldsymbol{P_4} \end{pmatrix} = \left(\begin{pmatrix} C_3 \\ C_4 \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod\ 26$$

$$\begin{pmatrix} \boldsymbol{P_3} \\ \boldsymbol{P_4} \end{pmatrix} = \left(\begin{pmatrix} M \\ T \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod\ 26$$

$$\begin{pmatrix} P_3 \\ P_4 \end{pmatrix} = \left(\begin{pmatrix} 12 \\ 19 \end{pmatrix} * \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \right) mod\ 26$$

$P_3 = \big((12 * 15) + (19 * 23)\big) \bmod 26$

$P_3 = \big((180) + (437)\big) \bmod 26$

$P_3 = (617) \bmod 26 = 19 = \mathrm{t}$

$P_4 = \big((12 * 8) + (19 * 9)\big) \bmod 26$

$P_4 = \big((96) + (171)\big) \bmod 26$

$P_4 = (267) \bmod 26 = 7 = \mathrm{h}$

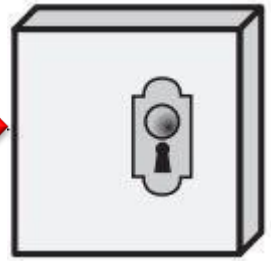
The Plaintext is : $P_1P_2P_3P_4$ → **"math"**

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

$$K^{-1} = \begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}$$

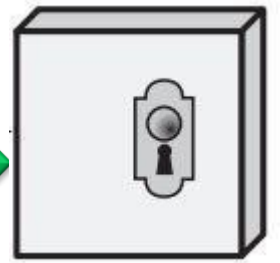
math

(Sender)



Encryption algorithm By using Hill Cipher

KUMT



Decryption algorithm By using Hill Cipher

math

(receiver)

Homework

1. By using Hill Cipher, encrypt the message "telecommunication" using the matrix key:

$$\mathbf{K} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

2. By using Hill Cipher, decrypt the message "GEACUFQZVEUQZKBWDK" using the matrix key:

$$\mathbf{K} = \begin{pmatrix} 16 & 1 \\ 7 & 54 \end{pmatrix}$$