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

Fourth Stage

Security

Lecture 5

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 3D Key.**

Hill Cipher when 3D Key

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 $n * m$ matrix, where n is the block size. System can be described as follows:

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

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

Where P → Plaintext

C → Ciphertext

K → Key

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

Hill Cipher when 3D Key

Alice

Sender

Bob

Receiver

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

K

Matrix

Encryption

K^{-1}

Inverse Matrix

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

Decryption

Cipher text

Example 1

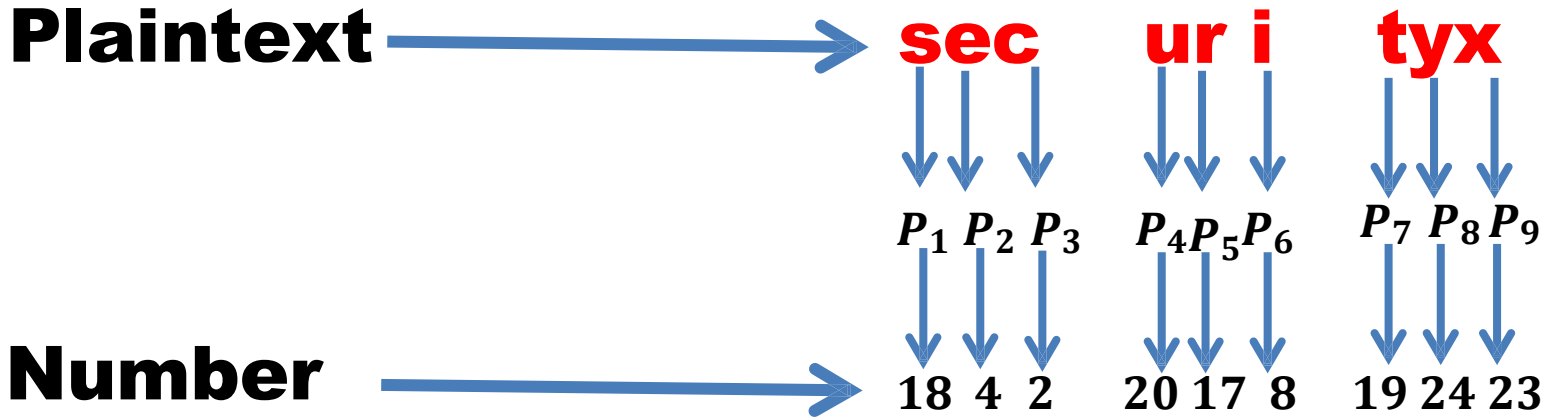
Encrypt and then decrypt the Plaintext "**Security**" by using **Hill Cipher** and by using the matrix key:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Ans:-

1. Encryption Algorithm

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



$P_1 = s = 18$
$P_2 = e = 4$
$P_3 = c = 2$

$$\begin{pmatrix} \mathbf{C_1} \\ \mathbf{C_2} \\ \mathbf{C_3} \end{pmatrix} = \left(\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{C_1} \\ \mathbf{C_2} \\ \mathbf{C_3} \end{pmatrix} = \left(\begin{pmatrix} s \\ e \\ c \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{C_1} \\ \mathbf{C_2} \\ \mathbf{C_3} \end{pmatrix} = \left(\begin{pmatrix} 18 \\ 4 \\ 2 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$C_1 = \big((18 * 17) + (4 * 17) + (2 * 5)\big) \bmod 26$$

$$C_1 = (384) \bmod 26$$

$$C_1 = 20 = U$$

$$C_2 = \big((18 * 21) + (4 * 18) + (2 * 21)\big) \bmod 26$$
$$C_2 = (492) \bmod 26$$
$$C_2 = 24 = Y$$

$$C_3 = \big((18 * 2) + (4 * 2) + (2 * 19)\big) \bmod 26$$
$$C_3 = (82) \bmod 26$$
$$C_3 = 4 = E$$

$$\mathbf{P_4 = u = 20}$$
$$\mathbf{P_5 = r = 17}$$
$$\mathbf{P_6 = i = 8}$$

$$\begin{pmatrix} \mathbf{C_4} \\ \mathbf{C_5} \\ \mathbf{C_6} \end{pmatrix} = \left(\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{C_4} \\ \mathbf{C_5} \\ \mathbf{C_6} \end{pmatrix} = \left(\begin{pmatrix} u \\ r \\ i \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{C_4} \\ \mathbf{C_5} \\ \mathbf{C_6} \end{pmatrix} = \left(\begin{pmatrix} 20 \\ 17 \\ 8 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$C_4 = \big((20 * 17) + (17 * 17) + (8 * 5)\big) \bmod 26$$

$$C_4 = (669) \bmod 26$$

$$C_4 = 19 = T$$

$$C_5 = \big((20 * 21) + (17 * 18) + (8 * 21)\big) \bmod 26$$

$$C_5 = (894) \bmod 26$$

$$C_5 = 10 = K$$

$$C_6 = \left((20 * 2) + (17 * 2) + (8 * 19)\right) \bmod 26$$
$$C_6 = (226) \bmod 26$$
$$C_6 = 18 = S$$

$$\mathbf{P_7 = t = 19}$$
$$\mathbf{P_8 = y = 24}$$
$$\mathbf{P_9 = x = 23}$$

$$\begin{pmatrix} \mathbf{C_7} \\ \mathbf{C_8} \\ \mathbf{C_9} \end{pmatrix} = \left(\begin{pmatrix} P_7 \\ P_8 \\ P_9 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{C_7} \\ \mathbf{C_8} \\ \mathbf{C_9} \end{pmatrix} = \left(\begin{pmatrix} t \\ y \\ x \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} C_7 \\ C_8 \\ C_9 \end{pmatrix} = \left(\begin{pmatrix} 19 \\ 24 \\ 23 \end{pmatrix} * \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \right) mod\ 26$$

$$C_7 = \big((19 * 17) + (24 * 17) + (23 * 5)\big) \bmod 26$$
$$C_7 = (846) \bmod 26$$
$$C_7 = 14 = O$$

$$C_8 = \big((19 * 21) + (24 * 18) + (23 * 21)\big) \bmod 26$$
$$C_8 = (1314) \bmod 26$$
$$C_8 = 14 = O$$

$$C_9 = \big((19 * 2) + (24 * 2) + (23 * 19)\big) \bmod 26$$
$$C_9 = (523) \bmod 26$$
$$C_9 = 3 = D$$

The Ciphertext is $C_1C_2C_3C_4\ C_5\ C_6\ C_7\ C_8\ C_9$ → "UYETKSOOD"

Inverse of the Matrix

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$$

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

1. We find the Determine of this matrix.

The determinant of a 3 × 3 matrix is defined by:

$$|A| = \begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a\begin{vmatrix} e & f \\ h & i \end{vmatrix} - b\begin{vmatrix} d & f \\ g & i \end{vmatrix} + c\begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

$$= aei + bfg + cdh - ceg - bdi - afh.$$

Inverse of the Matrix

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$$

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

1. We find the Determine of this matrix.

$$\boldsymbol{det(K)} = ([(K_{11} * K_{22} * K_{33}) + (K_{21} * K_{32} * K_{13}) + (K_{12} * K_{23} * K_{31})] - [(K_{31} * K_{22} * K_{13}) + (K_{21} * K_{12} * K_{33}) + (K_{11} * K_{32} * K_{23})])mod\ 26$$

$$\boldsymbol{det(K)} = ([(17 * 18 * 19) + (21 * 2 * 5) + (17 * 21 * 2)] - [(2 * 18 * 5) + (21 * 17 * 19) + (17 * 2 * 21)])\ mod\ 26$$

$$\boldsymbol{det(K)} = ([6738] - [7677])mod\ 26 = ([-939])mod\ 26 = -3\ mod\ 26$$

-3 + 26 = 23

$$\left(\boldsymbol{det(K)}\right)^{-1} = 17$$

2. We will find the sub determine of each element of the matrix.

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\begin{bmatrix} +\begin{vmatrix} 18 & 21 \\ 2 & 19 \end{vmatrix} & -\begin{vmatrix} 21 & 21 \\ 2 & 19 \end{vmatrix} & +\begin{vmatrix} 21 & 18 \\ 2 & 2 \end{vmatrix} \\ -\begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} & +\begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} & -\begin{vmatrix} 17 & 17 \\ 2 & 2 \end{vmatrix} \\ +\begin{vmatrix} 17 & 5 \\ 18 & 21 \end{vmatrix} & -\begin{vmatrix} 17 & 5 \\ 21 & 21 \end{vmatrix} & +\begin{vmatrix} 17 & 17 \\ 21 & 18 \end{vmatrix} \end{bmatrix} = \begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}$$

3. Then convert Row to Column.

$$\mathbf{K^T} = \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix}$$

4. Apply Hill Cipher Matrix Inverse equation.

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

$$K^{-1} = \left((17) * \begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \right) \bmod 26$$

$$K^{-1} = \begin{pmatrix} 5100 & -5321 & 4539 \\ -6069 & 5321 & -4284 \\ 102 & 0 & -867 \end{pmatrix} \bmod 26$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Verify

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

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

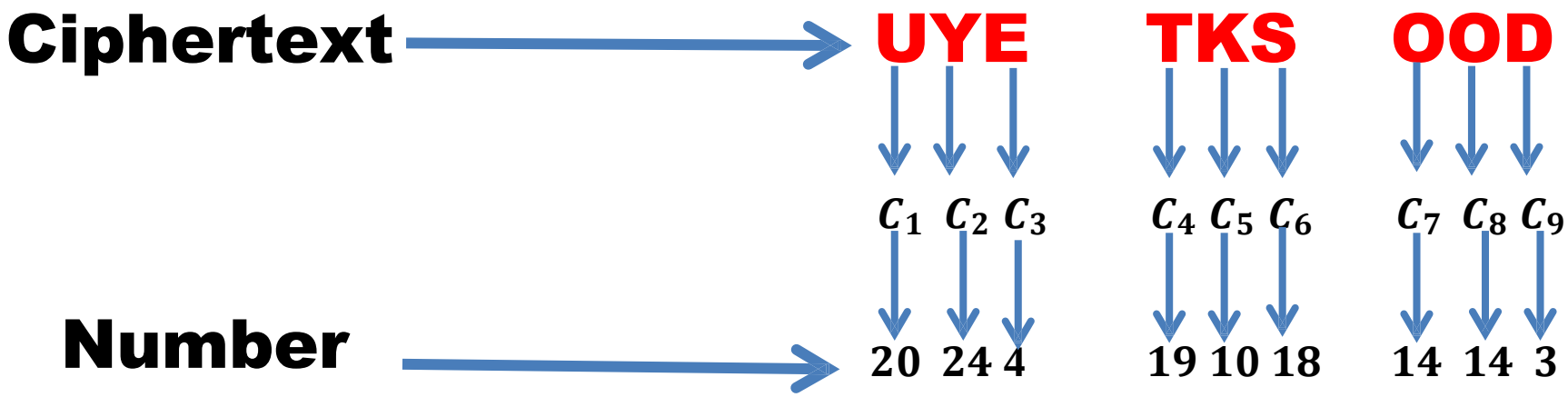
$$\left(\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} * \begin{pmatrix} \mathbf{4} & \mathbf{9} & \mathbf{15} \\ \mathbf{15} & \mathbf{17} & \mathbf{6} \\ \mathbf{24} & \mathbf{0} & \mathbf{17} \end{pmatrix}\right) \boldsymbol{mod\ 26}$$

$$\begin{pmatrix} (17*4)+(17*15)+(5*24) & (17*9)+(17*17)+(5*0) & (17*15)+(17*6)+(5*17) \\ (21*4)+(18*15)+(21*24) & (21*9)+(18*17)+(21*0) & (21*15)+(18*6)+(21*17) \\ (2*4)+(2*15)+(19*24) & (2*9)+(2*17)+(19*0) & (2*15)+(2*6)+(19*17) \end{pmatrix} mod\ 26$$

$$\begin{pmatrix} 443 & 442 & 422 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} mod\ 26 = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

2. Decryption Algorithm

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



$C_1 = U = 20$
$C_2 = Y = 24$
$C_3 = E = 4$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \left(\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{P_1} \\ \mathbf{P_2} \\ \mathbf{P_3} \end{pmatrix} = \left(\begin{pmatrix} \mathrm{U} \\ \mathrm{Y} \\ \mathrm{E} \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \boldsymbol{P_1} \\ \boldsymbol{P_2} \\ \boldsymbol{P_3} \end{pmatrix} = \left(\begin{pmatrix} 20 \\ 24 \\ 4 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) mod\ 26$$

$$\mathrm{P}_1 = \big((20 * 4) + (24 * 9) + (4 * 15)\big) \bmod 26$$

$$\mathrm{P}_1 = (356) \bmod 26$$

$$\mathrm{P}_1 = 18 = \mathrm{s}$$

$$\mathrm{P}_2 = \big((20 * 15) + (24 * 17) + (4 * 6)\big) \bmod 26$$

$$\mathrm{P}_2 = (732) \bmod 26$$

$$\mathrm{P}_2 = 4 = \mathrm{e}$$

$$P_3 = \big((20 * 24) + (24 * 0) + (4 * 17)\big) \bmod 26$$
$$P_3 = (548) \bmod 26$$
$$P_3 = 2 = c$$

$$\mathbf{C_4} = \mathbf{T} = \mathbf{19}$$
$$\mathbf{C_5} = \mathbf{K} = \mathbf{10}$$
$$\mathbf{C_6} = \mathbf{S} = \mathbf{18}$$

$$\begin{pmatrix} \mathbf{P_4} \\ \mathbf{P_5} \\ \mathbf{P_6} \end{pmatrix} = \left(\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{P_4} \\ \mathbf{P_5} \\ \mathbf{P_6} \end{pmatrix} = \left(\begin{pmatrix} T \\ K \\ S \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{P_4} \\ \mathbf{P_5} \\ \mathbf{P_6} \end{pmatrix} = \left(\begin{pmatrix} 19 \\ 10 \\ 18 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$P_4 = \big((19 * 4) + (10 * 9) + (18 * 15)\big) \bmod 26$$
$$P_4 = (436) \bmod 26$$
$$P_4 = 20 = \mathrm{u}$$

$$P_5 = \big((19 * 15) + (10 * 17) + (18 * 6)\big) \bmod 26$$
$$P_5 = (563) \bmod 26$$
$$P_5 = 17 = \mathrm{r}$$

$$P_6 = \big((19 * 24) + (10 * 0) + (18 * 17)\big) \bmod 26$$
$$P_6 = (762) \bmod 26$$
$$P_6 = 8 = \mathrm{i}$$

$$\mathbf{C_7 = O = 14}$$
$$\mathbf{C_8 = O = 14}$$
$$\mathbf{C_9 = D = 3}$$

$$\begin{pmatrix} \mathbf{P_7} \\ \mathbf{P_8} \\ \mathbf{P_9} \end{pmatrix} = \left(\begin{pmatrix} C_7 \\ C_8 \\ C_9 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{P_7} \\ \mathbf{P_8} \\ \mathbf{P_9} \end{pmatrix} = \left(\begin{pmatrix} O \\ O \\ D \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$\begin{pmatrix} \mathbf{P_7} \\ \mathbf{P_8} \\ \mathbf{P_9} \end{pmatrix} = \left(\begin{pmatrix} 14 \\ 14 \\ 3 \end{pmatrix} * \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \right) \bmod 26$$

$$P_7 = \big((14 * 4) + (14 * 9) + (3 * 15)\big) \bmod 26$$
$$P_7 = (227) \bmod 26$$
$$P_7 = 19 = t$$

$$P_8 = \big((14 * 15) + (14 * 17) + (3 * 6)\big) \bmod 26$$
$$P_8 = (466) \bmod 26$$
$$P_8 = 24 = y$$

$$P_9 = \big((14 * 24) + (14 * 0) + (3 * 17)\big) \bmod 26$$
$$P_9 = (387) \bmod 26$$
$$P_9 = 23 = x$$

The Plaintext is $P_1P_2P_3P_4\,P_5\,P_6\,P_7\,P_8\,P_9$ → **"securityx"**

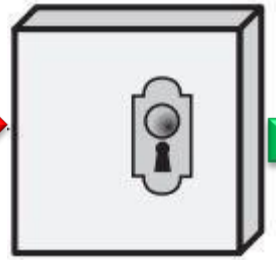
The Plaintext is $P_1P_2P_3P_4\,P_5\,P_6\,P_7\,P_8$ → **"security"**

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

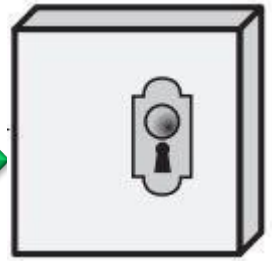
security

(Sender)



Encryption algorithm By using Hill Cipher

UYETKSOOD



Decryption algorithm By using Hill Cipher

security

(Receiver)

Homework

By using Hill Cipher, encrypt the message "telecommunication" using the Matrix Key :

$$K = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Find the Plaintext of the message by using Hill algorithm "VCOXTVASEULSXWQGTJISMDKT" with the matrix key:

$$K = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$