Q11) The plaintext "letusmeetnow" and the corresponding ciphertext "HBCD~~F~~FNOPIKLB" are given. You know that the algorithm is a hill cipher, but you don't know the size of the encryption matrix. Find the key matrix.

Ans 11) The length of the ciphertext and plaintext is 12. So, the different key lengths that are possible are 1, 2, 3, 4, 6, 12. The amount of plaintext/ciphertext pairs that we need to cipher key size m is m^2. So, for:-

1 : 1
2 : 4
3 : 9
4 : 16
~~5~~
6 : 36

pairs of ciphertext/plaintext are required.

We have only 12 ~~year~~ pairs of plaintext/ciphertext, so we can only check for key size m=1, 2, 3.

- $m=1$

We know that $C = P \cdot K$ in hill cipher where C is the resulting ciphertext matrix and P is the original plaintext ~~matt~~ matrix. We also know K is the Hill cipher encryption key where K is invertible and the operation $P = K \cdot K$ is in $\mathbb{Z}_{26}$ and congruent to mod(%) 26.

$C = P \cdot K$
$K = P^{-1} \cdot C$, here P^{-1} is the modular inverse of P congruent to 26. (mod)

This is not the correct encryption, hence the key we have selected [3] is incorrect and we will now search for a 2+2 key for Hill Cipher .

- 2x2

Let us consider Plaintext/Ciphertext pair LEUT/HBDI

We have

$$P = \begin{bmatrix} 11 & 4 \\ 20 & 19 \end{bmatrix} \quad C = \begin{bmatrix} 7 & 1 \\ 3 & 8 \end{bmatrix} \quad P^{-1} = \begin{bmatrix} 7 & 4 \\ 20 & 15 \end{bmatrix} \bmod 26$$

We get $K = P^{-1} . C$

$$= \begin{bmatrix} 7 & 4 \\ 20 & 15 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 3 & 8 \end{bmatrix} \% \; 26$$

$$= \begin{bmatrix} 61 & 39 \\ 185 & 140 \end{bmatrix} \% \; 26$$

$$= \begin{bmatrix} 9 & 13 \\ 3 & 10 \end{bmatrix}$$

We also have $K^{-1} \bmod 26 = \begin{bmatrix} 16 & 13 \\ 3 & 17 \end{bmatrix} \bmod 26$

So, this can ultimately be a key. We now encrypt our plaintext using this key and compare results with the given ciphertext

$$C = \begin{bmatrix} 11 & 4 \\ 19 & 20 \\ 18 & 12 \\ 4 & 4 \\ 19 & 13 \\ 14 & 22 \end{bmatrix} \begin{bmatrix} 9 & 13 \\ 3 & 10 \end{bmatrix} = \begin{bmatrix} 7 & 1 \\ 23 & 5 \\ 16 & 16 \\ 22 & 14 \\ 2 & 13 \\ 10 & 12 \end{bmatrix} = \text{HBXFQQWOCNKM}$$

Not very plaintext matrix is investible, but for an invertible pair the $K = P^{-1} \cdot C$ is solvable and the resulting matrix for K should also be modular matrix investible.

If the resulting key matrix is not invertible, then no solution exists for that particular key size.

We can prove this by proof of contradiction. Let us assume that a key exists for Hill cipher of size m that converts plaintext P to ciphertext C, hence

$$C = P \cdot K$$

$K = P^{-1} \cdot C$ and if we take $P^{-1} \cdot C$, the result we get must be that key and if the result isn't investible, then the key we have obtained was never a key to begin with.

Now, for $\underline{m=1}$, let us assume the plaintext / ciphertext pair as: L/H. We get

$P = [11] \quad C = [7] \quad P^{-1} = [11]^{-1} = [19] \bmod 26$

$$K = P^{-1} \cdot C$$
$$= [19][7]$$
$$= 3$$

Now, let us encrypt the plaintext message using this key and see encrypted message

$C = [3][11 \; 4 \; 19 \; 20 \; 18 \; 12 \; 4 \; 4 \; 19 \; 13 \; 14 \; 22]$

$C = [7 \; 12 \; 5 \; 8 \; 2 \; 10 \; 12 \; 12 \; 5 \; 13 \; 16 \; 14]$

$= [H \; M \; F \; I \; C \; K \; M \; M \; F \; N \; Q \; O]$

As the ciphertext we are receiving is not the correct ciphertext, we conclude that a key size of 2 hasn't been used for encrypting the data.

• 3×3

We have plaintext and ciphertext as

$$P = [11 \ 4 \ 19 \ 20 \ 18 \ 12 \ 4 \ 4 \ 19 \ 13 \ 14 \ 22]$$

It is arranged in blocks of 3 as follows:-

$$\begin{bmatrix} 11 & 4 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix} \cdot K = \overset{\text{ciphertext}}{\begin{bmatrix} 7 & 1 & 2 \\ 3 & 5 & 13 \\ 14 & 15 & 8 \\ 10 & 11 & 1 \end{bmatrix}}$$

We have to take 3 blocks of ciphertext / plaintext to find the key K such that P^{-1} exists and also K^{-1} exists, and resulting decryption/encryption is a match.

Let us take matrix block

$$P = \begin{bmatrix} 11 & 14 & 19 \\ 20 & 18 & 12 \\ 4 & 4 & 19 \end{bmatrix}$$

Here P^{-1} doesn't exist as $|P| = 2058$, which isn't coprime in 26 and hence a modular inverse doesn't exist.

Now, we take

$$P = \begin{bmatrix} 11 & 14 & 19 \\ 20 & 18 & 12 \\ 13 & 14 & 22 \end{bmatrix}$$

$|P| = 2246$

2246 isn't coprime with 26, hence modular matrix inverse doesn't exist.

Let us now consider:-

$$P = \begin{bmatrix} 11 & 4 & 19 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix}$$

$|P| = -1246$

-1246 is not coprime with 26 and hence this matrix has no modular inverse and hence can't be used to find key. We now consider

$$P = \begin{bmatrix} 20 & 18 & 12 \\ 4 & 4 & 19 \\ 13 & 14 & 22 \end{bmatrix} \quad |P| = -650$$

-650 ~~is~~ isn't coprime with 26 and hence has no modular inverse. So, ~~the~~ the key is definitely not 3×3. We conclude either that the key size is higher 4×4, 6×6 or 12×12 or a key doesn't exist.