Date: _____

Name: Nashra Ghaffar

Roll No: CT-20032 (Sec A)

Course Code: CT-486

Hill Cipher Assignment.

Q: Calculate the Hill Cipher Decayption key for a 3 x 3 matrix.

Let's assume,

Plaintext = NEDUET.

Cipher text = VDJBUZ

Secret key = $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

The decryption key for the given cipher will be:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Let's see how to calculate it:

Date: _____

Let,

$$A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

(1) Finding determinant of matrix A.

$$= 6\{(16\times15)-(17\times10)\} - 13\{(24\times15)-(17\times1)\} + 20\{(24\times10)-(16\times1)\}$$

$$\det(A) = 420 - 4459 + 4480$$

$$\boxed{\det(A) = 441}$$

(2) Finding modular inverse of A.

$$441 \cdot x \bmod 26 = 1.$$

Here, assume, $\boxed{x = 25}$

So,

$$(441 \times 25) \bmod 26 = 1.$$

(3) Finding adjugate of A.

Adjugate of $A = C^t$ (Transpose of C)

$$C = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix}$$

where C = cofactors of matrix A.

Date: _____

$C_{11} = (16 \times 15) - (17 \times 10)$

$C_{11} = 70$

$C_{12} = (13 \times 15) - (10 \times 20)$

$C_{12} = -5$

$C_{13} \quad (13 \times 17) - (20 \times 16)$

$C_{13} \quad -99$

$C_{21} \quad (24 \times 15) - (17 \times 1)$

$C_{21} \quad 343$

$C_{22} \quad (6 \times 15) - (20 \times 1)$

$C_{22} \quad 70$

$C_{23} \quad (6 \times 17) - (20 \times 24)$

$C_{23} \quad -378$

$C_{31} \quad (24 \times 10) - (16 \times 1)$

$C_{31} \quad 224$

$C_{32} \quad (6 \times 10) - (13 \times 1)$

$C_{32} \quad 47$

$C_{33} \quad (6 \times 16) - (24 \times 13)$

$C_{33} \quad -216$

Adjugate $A = \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$

Date: _____

(4) $(x \cdot Adj(A)) \bmod 26$.

$$25 \begin{bmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{bmatrix}$$

$$x \cdot Adj(A) = \begin{bmatrix} 1750 & -8575 & 5600 \\ 125 & 1750 & -1175 \\ -2475 & 9450 & -5400 \end{bmatrix}$$

$$x \cdot Adj(A) \bmod 26 = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

So, the decryption key is:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$