FALL SEMESTER 2020-21
MAT3004

APPLIED LINEAR ALGEBRA

DIGITAL ASSIGNMENT-1

NAME: VIBHU KUMAR SINGH
REG NO: 19BCE0215
TEACHER: PADMA R.

Instructions: Write in neat hand writing both the questions with your name and registration number written in each sheet. The total number of pages should not exceed 6 pages**. Only pdf files should be uploaded in vtop. No word document**. First question is compulsory for all.

1. Explain the Hill cipher.

A1. Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26.
Often a simple scheme:

$$A=0, B=1, C=2 \dots, Z=25$$

is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letter (considered as an n-component vector) is multiplied by the inverse of the matrix used for encryption.
To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

General formula for encryption:

$$\boxed{C = KP \pmod N}$$

C: Cipher Text
K: Key matrix
P: Plain Text

General formula for decryption:

$$\boxed{P = K^{-1}C \pmod N}$$

C: Cipher Text
K: Key matrix
P: Plain Text.

classmate

2. The six sets of questions are meant for the six groups of students mentioned below the problem. You can consult among your group and do.
We denote the number of symbols by N and the matrix by A and given below the cipher text that has been encrypted with the matrix A mod N. Find the plain text.

II) N=37, A = ^7 3]Encoding : 0 ^ 0, .,9 ^ 9,A ^ 10,$\ldots Z$ ^ 35, *blank* ^ 36

Cipher text: AP4FQXFN1O34M6JWR8

19BCE0215

A2. II) $N=37$, $A=\begin{bmatrix}5 & 2\\ 7 & 3\end{bmatrix}$, encoding $0\leftrightarrow 0 \ldots 9\leftrightarrow 9$, $A\leftrightarrow 10 \ldots Z\leftrightarrow 35$, Blank $\leftrightarrow$ 36.

Given
Cipher Text : AP4FQXFN1034M6JWR8

To find : Plain Text using hill cipher decryption.

$$A^{-1} = \frac{1}{|A|}\,\mathrm{adj}(A) = \begin{bmatrix}3 & -2\\ -7 & 5\end{bmatrix} \quad \because (|A|=1)$$

Since the Key(A) is 2X2 matrix, we will group the cipher text in group of 2.

$\Rightarrow$ Cipher Text : (AP)(4F)(QX)(FN)(10)(34)(M6)(JW)(R8)

$\hookrightarrow$ According to the above cipher Text :

(i) $(AP) \equiv \begin{bmatrix}3 & -2\\ -7 & 5\end{bmatrix}\begin{bmatrix}10\\ 25\end{bmatrix} \pmod{37}$ $\quad (P = K^{-1}C \bmod 37)$

$$\equiv \begin{bmatrix}-20\\ 55\end{bmatrix} \pmod{37} = \begin{bmatrix}17\\ 18\end{bmatrix} \Rightarrow \begin{bmatrix}H\\ I\end{bmatrix} \text{ (decoded)}$$

$\boxed{(AP) \equiv (HI)}$

classmate

19BCE0215

$$= \begin{bmatrix} -45 \\ 113 \end{bmatrix} (\text{mod } 37) = \begin{bmatrix} 29 \\ 2 \end{bmatrix} = \begin{bmatrix} T \\ 2 \end{bmatrix} \text{ (decoded)}$$

$$= \boxed{(10) \equiv (T2)}$$

(vi) $(34) \equiv \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix} (\text{mod } 37)$

$$= \begin{bmatrix} 1 \\ -1 \end{bmatrix} (\text{mod } 37) = \begin{bmatrix} 1 \\ 36 \end{bmatrix} = \begin{bmatrix} 1 \\ \text{(Blank)} \end{bmatrix} \text{ (decoded)}$$

$$\boxed{(34) \equiv (1\_)}$$

(vii) $(M6) = \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 22 \\ 6 \end{bmatrix} (\text{mod } 37)$

$$= \begin{bmatrix} 54 \\ -124 \end{bmatrix} (\text{mod } 37) = \begin{bmatrix} 27 \\ 24 \end{bmatrix} = \begin{bmatrix} H \\ O \end{bmatrix} \text{ (decoded)}$$

$$\boxed{(M6) \equiv (HO)}$$

(viii) $(JW) = \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 19 \\ 32 \end{bmatrix} (\text{mod } 37)$

$$= \begin{bmatrix} -7 \\ 27 \end{bmatrix} (\text{mod } 37) = \begin{bmatrix} 30 \\ 27 \end{bmatrix} = \begin{bmatrix} U \\ R \end{bmatrix} \text{ (decoded)}$$

$$\boxed{(JW) \equiv (UR)}$$

(ix) $(R8) = \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 27 \\ 8 \end{bmatrix} (\text{mod } 37)$

19BLE0415

(ii) $(4F) \equiv \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 4 \\ 15 \end{bmatrix} \pmod{37}$

$= \begin{bmatrix} -18 \\ 47 \end{bmatrix} \pmod{37} = \begin{bmatrix} 19 \\ 10 \end{bmatrix} \Rightarrow \begin{bmatrix} J \\ A \end{bmatrix}$ (decoded)

$\boxed{(4F) \equiv (JA)}$

(iii) $(QX) \equiv \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 26 \\ 33 \end{bmatrix} \pmod{37}$

$= \begin{bmatrix} 12 \\ -17 \end{bmatrix} \pmod{37} = \begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$ (decoded)

$\boxed{(QX) \equiv (CK)}$

(iv) $(FN) = \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} \pmod{37}$

$= \begin{bmatrix} -1 \\ 10 \end{bmatrix} \pmod{37} = \begin{bmatrix} 36 \\ 10 \end{bmatrix} = \begin{bmatrix} \text{(Blank)} \\ A \end{bmatrix}$ (decoded)

$\boxed{(FN) \equiv (\_A)}$

(V) $(1O) \equiv \begin{bmatrix} 3 & -2 \\ -7 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 24 \end{bmatrix} \pmod{37}$

$$= \begin{bmatrix} 65 \\ -149 \end{bmatrix} \pmod{37} = \begin{bmatrix} 28 \\ 36 \end{bmatrix} = \begin{bmatrix} S \\ \text{(Blank)} \end{bmatrix} \text{ (decoded)}$$

$$\boxed{(R8) = (S\ \_)}$$

<u>Result</u>: The decoded plain text for the cipher text is:

H1JACK_AT21_HOURS_

$\boxed{19BCE0215}$.