ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

SOME APPLICATIONS OF LINEAR ALGEBRA IN CRYPTOGRAPHY

G.Venkata Subbaiah*, Prof. K. Rama Krishna Prasad
*Lecturer in Mathematics, Government College for Men Kadapa.
Department of Mathematics, S.V. University, Tirupati.

Keywords: Encryption, decryption, algorithm, plaintext, cipher text.

ABSTRACT
In this paper the main cryptography technique we will use is caesar cipher involving replacing each letter of the alphabet with the letter standing 3 places further down the alphabet. Here the encryption algorithm takes plaintext letters as input, and produces cipher text letters for them.

INTRODUCTION

We define encryption scheme.

An encryption scheme or cryptosystem is a tuple (P, C, K, E, D) with the following properties.

1. P is a set. It is called the plaintext space. Its elements are called plain texts.
2. C is a set. It is called the ciphertext space. Its elements are called cipher texts.
3. K is a set. It is called the key space. Its elements are called keys.
4. E= $\{E_k : k \varepsilon K\}$ is a family of functions $E_k : P \rightarrow C$. its elements are called encryption functions.
5. D= $\{D_k : k \varepsilon K\}$ is a family of functions $D_k : P \rightarrow C$. Its elements are called decryption functions.
6. For each e ε K there is d εK such that $D_d(E_e(p))=p$ for all p ε P.

- Cryptography is the study of the techniques of writing and decoding message in code.
- Cipher – A procedure that will render a message unintelligible to the recipient. Used to also recreate the original message.
- Plaintext-the message or information that is being encrypted.
- Ciphertext- the message or information that is created after the cipher has been used.
- Examples of encryption:
  Shift cipher, substitution, Transformation

Summary of Application in Linear Algebra

- A matrix can be used as a cipher to encrypt a message.
  The matrix must be invertible for use in decrypting.
- Cipher matrix can be as sample as a 3x3 matrix composed of Radom integers.
- In order to encrypt plaintext, each character in the plaintext must be denoted with a numerical value and placed into a matrix.
- These numbers can range in value, but an example is using 1-26 to represent A to Z and 27 to represent a space.
- This matrix is multiplied with the cipher matrix to form a new matrix containing the ciphertext message.

Encrypting a message;

- Each character of the plaintext is given a numerical values as stated before.
- These values are then separated into vectors, S.T. the number of rows of each vector is equivalent to the number of rows the cipher matrix.
- Values are placed into each vector one at a time, going down a row for each values. A vector is filled by the plaintext then the remaining entries will hold the values for space.
- The vectors are then augmented to form a matrix that contains the plaintext.
- The plaintext matrix is then multiplied with the cipher matrix to create the ciphertext matrix.

The encryption process. We can summarize the encryption which is the process of converting plaintext into cipher text in the following steps.

I. Choose a pxp matrix A which is invertible, where ‘p’ may have be depends on the length of the message that needs to be encrypted.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

II. Change each plaintext to its numerical value units as in table below

A	B	C	D	E	F	G	H	I	J
3	4	5	6	7	8	9	10	11	12
K	L	M	N	O	P	Q	R	S	T
13	14	15	16	17	18	19	20	21	22
U	V	W	X	Y	Z				
23	24	25	0	1	2				

III. Form the px1 column vector P, having these numerical values as its entries.

IV. Get each Cipher text vector C by multiplying A with P_1 and convert each entry of the ciphertext vector to its letter in the alphabet. The encryption algorithm of this method is:

$C \cong AP \bmod N$

Where C is the column vector of the numerical values of ciphertext, P is the column vector of the numerical values of plaintext, A is a pxp matrix, which is the key of the algorithm, (this matrix must be invertible because we need the inverse of this matrix for the decryption process) and N is the number of letters of the alphabet in the cryptography.

The decryption process:

The decryption which is the process of converting the ciphertext into plain text can also be summarized in the following steps:

I. Get the inverse of the matrix A say A^{-1}

II. Change each cipher text to its numerical value.

III. Put each cipher text in a px1 column vector say C.

IV. Get each plain text vector by multiplying A^{-1} with C and convert each plaintext vector to its letter in the alphabet. The decryption algorithm of this method is

$P = A^{-1} C \bmod N$

Where A^{-1} in the inverse of the matrix A.

In General, if $A=\begin{pmatrix} a_{11} & .... & a_{1n} \\ ... & .... & ... \\ a_{n1} & .... & a_{nn} \end{pmatrix} and\ p=\begin{pmatrix} p_{11} \\ ... \\ p_{n1} \end{pmatrix}$ then in the encryption process, we get

$C= AP \bmod N.$

$$\rightarrow \begin{pmatrix} c_{11} \\ ... \\ c_{n1} \end{pmatrix} \begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & ... & ... \\ a_{n1} & .... & a_{nn} \end{pmatrix} and\ p=\begin{pmatrix} p_{11} \\ ... \\ p_{n1} \end{pmatrix} ModN$$

Here when the size of the matrix A increases we will have following advantages.

1) The cryptography process will be more complex and more difficult to decade.
2) The number of column vector will decreases and we can encode any message consisting for example of 7 letters by using a (7x7) matrix in only one step. But there is one problem here, i.e it's not easy to get the inverse of the matrix used in the encryption process as its size increases.

We will give several other ways of using Ceasar cipher technique for encryption as given below

In the Caesar cipher, since the key used to encode (or) decode any message in a matrix we can use the associative property of matrices to make the coding process more complex and more secure. Therefore if we have two invertible matrices A, B, and a plaintext column vector P, the general case in explained below.

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

Given A= $\rightarrow \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots. & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} p = \begin{pmatrix} p_{11} \\ \dots \\ p_{n1} \end{pmatrix}$, the encryption algorithm is.

C= ABP=A(BP)= $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots. & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \dots \\ p_{n1} \end{pmatrix} = \begin{pmatrix} c_{11} \\ \dots \\ c_{n1} \end{pmatrix}$, mod N the decryption algorithm on the other hand is

$P=(AB)^{-1}. C=B^{-1}A^{-1}C=B^{-1}(A^{-1}C) \bmod N$

In this way, we get a new cipher column vector C because the matrix multiplication operation is an associative. Here, we also use the fact that $(XY)^{-1}=Y^{-1}. X^{-1}$
Note also that:

$(XY)^{-1} = Y^{-1}X^{-1} = X^{-1}Y^{-1}$ if and only if X and Y commute .Here we should be careful as matrix multiplication in not always commutative.

In this case we can use' n' number of invertible matrices to encode (or) decode any measure and the steps will be the same. This means that, it we have the invertible matrices A,B,C,….,M then the encryption algorithm will be C= (ABC—M) P Mod N.

$$\begin{pmatrix} c_{11} \\ \dots \\ c_{n1} \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots. & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \dots \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \dots & \dots & \dots \\ m_{n1} & \dots & m_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \dots \\ p_{n1} \end{pmatrix} \bmod N$$

Here the decryption algorithm is
P= (ABC…M) $^{-1}$ C mod N.

We can me the affine cipher technique to make the Caesar cipher more complex. Encryption algorithm here is given as
C= AP+B (mod N).

$$\begin{pmatrix} c_{11} \\ \dots \\ c_{n1} \end{pmatrix} \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots. & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} p_{11} \\ \dots \\ p_{n1} \end{pmatrix} + \begin{pmatrix} b_{11} \\ \dots \\ b_{n1} \end{pmatrix} (\bmod N) \text{ (mod N)}$$

Where A is an invertible matrix b is a column vector like the vector c and p.
For the decryption.

$P= A^{-1}C - A^{-1}B = A^{-1}(C-B) \pmod N$

By using the following algorithm to encrypt any message we will get more complex process.
C= (AB-M) P+K (mod N)

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

$$\begin{pmatrix} c_{11} \\ \dots \\ c_{n1} \end{pmatrix}\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots. & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots. & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}\dots\begin{pmatrix} m_{11} & \dots & m_{1n} \\ \dots & \dots. & \dots \\ m_{n1} & \dots & m_{nn} \end{pmatrix}\begin{pmatrix} p_{11} \\ \dots \\ p_{n1} \end{pmatrix}+\begin{pmatrix} k_{11} \\ \dots \\ k_{n1} \end{pmatrix}(\mathrm{mod}\, N)$$

The decryption have work as bellow

P= (AB-M) $^{-1}$ (C-K) (Mod N)

Here are some examples to illustrate the above facts

Examples:

1. Encode the message **"SAVEME"** by using Caesar cipher algorithm where the matrix is A= $\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$

Sol: We use the table below to convert letters in the message to the numerical values.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	5	6	7	8	9	10	11	12	13	14	15	16	17
O	P	Q	R	S	T	U	V	W	X	Y	Z		
18	19	20	21	22	23	24	25	0	1	2	3		

Put also number 'O' for the space between words. Group the plaintext letter into pairs and add o fill out the last pair.

S	A	V	E	M	E	
11	4	25	8	0	8	0

C= AP mod N.

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix}=\begin{pmatrix} 11+8 \\ 33+4 \end{pmatrix}(\mathrm{mod}\ 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 11 \\ 4 \end{pmatrix}=\begin{pmatrix} 11+8 \\ 33+4 \end{pmatrix}(mod\ 26)=\begin{pmatrix} 19 \\ 1\ 1 \end{pmatrix}(Mod 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 25 \\ 8 \end{pmatrix}=\begin{pmatrix} 25+16 \\ 75+8 \end{pmatrix}(\mathrm{mod}\, 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 25 \\ 8 \end{pmatrix}=\begin{pmatrix} 41 \\ 83 \end{pmatrix}(\mathrm{mod}\ 26)=\begin{pmatrix} 15 \\ 6 \end{pmatrix}(\mathrm{mod}\ 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 16 \end{pmatrix}=\begin{pmatrix} 0+32 \\ 0+16 \end{pmatrix}(\mathrm{mod}\ 26)=\begin{pmatrix} 6 \\ 10 \end{pmatrix}(\mathrm{mod}\ 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 8 \\ 0 \end{pmatrix}=\begin{pmatrix} 8+0 \\ 24+0 \end{pmatrix}(Mod\ 26)$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}\begin{pmatrix} 8 \\ 0 \end{pmatrix}=\begin{pmatrix} 8 \\ 24 \end{pmatrix}(Mod\ 26)=\begin{pmatrix} 18 \\ 2 \end{pmatrix}(\mathrm{mod}\ 26)$$

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

Now the message become "PHLCCGOY"

19	11	15	6	6	10	18	2
P	H	L	C	C	G	O	Y

2) Encode the following measure by using the matrices.

A=$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}, B\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}$ (I AM IN CLASS)

Sol: Put the plain text message in pairs: Change the letters to their numerical values by using the following table and put o instead of a space between words:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	5	6	7	8	9	10	11	12	13	14	15	16	17
O	P	Q	R	S	T	U	V	W	X	Y	Z		
18	19	20	21	22	23	24	25	0	1	2	3		

$Let \quad get \quad P_1=\begin{pmatrix}12\\ 0\end{pmatrix}, P_2=\begin{pmatrix}4\\ 16\end{pmatrix}, P_3=\begin{pmatrix}0\\ 12\end{pmatrix}, P_4=\begin{pmatrix}17\\ 0\end{pmatrix}, P_5=\begin{pmatrix}6\\ 15\end{pmatrix}$

$P_6=\begin{pmatrix}4\\ 22\end{pmatrix}, P_7=\begin{pmatrix}22\\ 0\end{pmatrix}$

Here we put ' O' for the space between words therefore

C ≅ ABP mod N

$$\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}\begin{pmatrix}12\\ 0\end{pmatrix}=\begin{pmatrix}3+4 & 1+8\\ 9+2 & 3+4\end{pmatrix}\begin{pmatrix}12\\ 0\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}\begin{pmatrix}12\\ 0\end{pmatrix}=\begin{pmatrix}7 & 9\\ 11 & 7\end{pmatrix}\begin{pmatrix}12\\ 0\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}84+0\\ 132+0\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}84\\ 132\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}6\\ 2\end{pmatrix}(\text{mod } 26))$$

$$\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}\begin{pmatrix}4\\ 16\end{pmatrix}=\begin{pmatrix}3+4 & 1+8\\ 9+2 & 3+4\end{pmatrix}\begin{pmatrix}14\\ 16\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}\begin{pmatrix}4\\ 16\end{pmatrix}=\begin{pmatrix}7 & 9\\ 11 & 7\end{pmatrix}\begin{pmatrix}14\\ 16\end{pmatrix}(\text{mod } 26))$$

$$=\begin{pmatrix}28+144\\ 44+112\end{pmatrix}(\text{mod } 26))=\begin{pmatrix}172\\ 156\end{pmatrix}(\text{mod } 26))=\begin{pmatrix}16\\ 0\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 1\\ 2 & 4\end{pmatrix}\begin{pmatrix}0\\ 12\end{pmatrix}=\begin{pmatrix}3+4 & 1+8\\ 9+2 & 3+4\end{pmatrix}\begin{pmatrix}0\\ 12\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7 & 9\\ 11 & 7\end{pmatrix}\begin{pmatrix}0\\ 12\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}0+96\\ 0+84\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}18\\ 6\end{pmatrix}(\text{mod } 26)$$

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

$$\begin{pmatrix}1&2\\3&1\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix}\begin{pmatrix}17\\0\end{pmatrix}=\begin{pmatrix}3+4&1+8\\9+2&3+4\end{pmatrix}\begin{pmatrix}7\\10\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7&9\\11&7\end{pmatrix}\begin{pmatrix}17\\0\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}119+90\\187+10\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}119\\187\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}15\\5\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1&2\\3&1\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix}\begin{pmatrix}0\\12\end{pmatrix}=\begin{pmatrix}3+4&1+8\\9+2&3+4\end{pmatrix}\begin{pmatrix}0\\12\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7&9\\11&7\end{pmatrix}\begin{pmatrix}0\\12\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}0+96\\0+84\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}18\\6\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1&2\\3&1\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix}\begin{pmatrix}16\\15\end{pmatrix}=\begin{pmatrix}3+4&1+8\\9+2&3+4\end{pmatrix}\begin{pmatrix}6\\15\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7&9\\11&7\end{pmatrix}\begin{pmatrix}6\\15\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}42+135\\66+105\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}177\\171\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}21\\15\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1&2\\3&1\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix}\begin{pmatrix}16\\15\end{pmatrix}=\begin{pmatrix}3+4&1+8\\9+2&3+4\end{pmatrix}\begin{pmatrix}4\\22\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7&9\\11&7\end{pmatrix}\begin{pmatrix}4\\22\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}28+198\\44+154\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}28+198\\44+154\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}226\\198\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}18\\16\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}1&2\\3&1\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix}\begin{pmatrix}22\\0\end{pmatrix}=\begin{pmatrix}3+4&1+8\\9+2&3+4\end{pmatrix}\begin{pmatrix}22\\0\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}7&9\\11&7\end{pmatrix}\begin{pmatrix}22\\0\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}154+0\\242+0\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}154\\242\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}24\\8\end{pmatrix}(\text{mod } 26)$$

Then the changing every value to the letter, the cipher text message becomes "CYMWOCLBRLOMUE"

6	2	16	0	18	6	15	5	21	15	18	16	24	8
C	Y	M	W	O	C	L	B	R	L	O	M	U	E

3).Try to encode " INDIAN " by using the algorithm C= AP+B (Mode 26)

$$when\ A=\begin{pmatrix}4&3\\2&5\end{pmatrix}, B=\begin{pmatrix}3\\4\end{pmatrix}$$

By using the table :

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

A	B	C	D	E	F	G	H	I	J	K	L	M	N
4	5	6	7	8	9	10	11	12	13	14	15	16	17
O	P	Q	R	S	T	U	V	W	X	Y	Z		
18	19	20	21	22	23	24	25	0	1	2	3		

I N D I A N
12 17 7 12 4 7

Then C= AP+B (mod N)

$$\begin{pmatrix}4 & 3\\ 2 & 5\end{pmatrix}\begin{pmatrix}12\\17\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}=\begin{pmatrix}48+51\\24+85\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}99\\109\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}102\\113\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}24\\9\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}4 & 3\\ 2 & 5\end{pmatrix}\begin{pmatrix}7\\12\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}=\begin{pmatrix}28+36\\14+60\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}64\\74\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)=\begin{pmatrix}67\\78\end{pmatrix}+(\text{mod } 26)=\begin{pmatrix}15\\0\end{pmatrix}(\text{mod } 26)$$

$$\begin{pmatrix}4 & 3\\ 2 & 5\end{pmatrix}\begin{pmatrix}4\\17\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}=\begin{pmatrix}16+51\\8+85\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)$$

$$=\begin{pmatrix}67\\93\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}(\text{mod } 26)\ =\begin{pmatrix}70\\97\end{pmatrix}+(\text{mod } 26)=\begin{pmatrix}18\\19\end{pmatrix}(\text{mod } 26)$$

$\therefore$ INDIAN =UFLWOP

3) De code the message " I T A P U R I T Y T I S R E V I N U A R A W S E T A K N E V I R S " by using Caesar cipher Algorithm and the inverse of the matrix

$$A=\begin{pmatrix}1 & 3 & 3\\ 1 & 4 & 3\\ 1 & 3 & 4\end{pmatrix}$$

Sol: since $A=\begin{pmatrix}1 & 3 & 3\\ 1 & 4 & 3\\ 1 & 3 & 4\end{pmatrix}$ by using matrix inversion method

$A^{-1}=\begin{pmatrix}7 & -3 & -3\\ -1 & 1 & 0\\ -1 & 0 & 1\end{pmatrix}$ Now, put the cipher text into groups where each group consists of three letters. Find

The numerical value of each letter from the table above therefore.

Now put the cipher text

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}12\\23\\4\end{pmatrix}\begin{pmatrix}84-69-12\\-12+23+0\\-12+0+4\end{pmatrix}(\text{mod }26)$$

$$=\begin{pmatrix}3\\11\\-8\end{pmatrix}(\text{mod }26)=\begin{pmatrix}3\\11\\18\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}19\\24\\21\end{pmatrix}\quad\begin{pmatrix}133-72-63\\-12+24+0\\-12+0+21\end{pmatrix}(\text{mod }26)$$

$$=\begin{pmatrix}2\\5\\2\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}12\\23\\2\end{pmatrix}\begin{pmatrix}84-69-6\\-12+23+0\\-12+0+2\end{pmatrix}(\text{mod }26)$$

$$=\begin{pmatrix}9\\11\\-10\end{pmatrix}(\text{mod }26)=\begin{pmatrix}9\\11\\16\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}23\\12\\22\end{pmatrix}\quad\begin{pmatrix}161-36-66\\-23+12+0\\-23+0+22\end{pmatrix}(Mod\,26)$$

$$=\begin{pmatrix}59\\-11\\-1\end{pmatrix}(\text{mod }26)=\begin{pmatrix}7\\15\\25\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}21\\8\\25\end{pmatrix}=\begin{pmatrix}147-24-75\\-21+8+0\\-21+0+25\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}48\\-13\\4\end{pmatrix}(\text{mod }26)=\begin{pmatrix}22\\13\\4\end{pmatrix}(\text{mod }26)$$

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

$$\begin{pmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 12 \\ 17 \\ 24 \end{pmatrix} = \begin{pmatrix} 84-51-72 \\ -12+17+0 \\ -12+0+24 \end{pmatrix} (\text{mod } 26)$$

$$\begin{pmatrix} -39 \\ 5 \\ 12 \end{pmatrix} (\text{mod } 26) \begin{pmatrix} 13 \\ 5 \\ 12 \end{pmatrix} (\text{mod } 26)$$

$$\begin{pmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 4 \\ 21 \\ 4 \end{pmatrix}\begin{pmatrix} 28 & -63 & -12 \\ -4+21 & +0 \\ -4 & +0 & +4 \end{pmatrix} (\text{mod } 26)$$

$$= \begin{pmatrix} -47 \\ 17 \\ 0 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 21 \\ 17 \\ 0 \end{pmatrix} (\text{mod } 26)$$

$$\begin{pmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 22 \\ 8 \end{pmatrix} = \begin{pmatrix} 0-66-24 \\ -0+22+0 \\ -0+0+8 \end{pmatrix} (\text{mod } 26)$$

$$= \begin{pmatrix} -90 \\ 22 \\ 8 \end{pmatrix} \text{mod } 26)$$

$$= \begin{pmatrix} 12 \\ 22 \\ 8 \end{pmatrix} \text{mod } 26)$$

ISSN 2349-6193
Impact Factor (PIF): 2.243

IJESMR
International Journal OF Engineering Sciences & Management Research

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}23\\4\\14\end{pmatrix}=\begin{pmatrix}161-12-42\\-23+4+0\\123+0+14\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}107\\-19\\-9\end{pmatrix}(\text{mod }26)=\begin{pmatrix}4\\7\\17\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}17\\8\\25\end{pmatrix}=\begin{pmatrix}119-24-75\\-17+8+0\\-17+0+25\end{pmatrix}(\text{mod }26)$$

$$=\begin{pmatrix}20\\-9\\8\end{pmatrix}\text{mod }26)=\begin{pmatrix}20\\17\\8\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7&-3&-3\\-1&1&0\\-1&0&1\end{pmatrix}\begin{pmatrix}12\\21\\22\end{pmatrix}\begin{pmatrix}84-63-66\\-12+21+0\\-12+0+22\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}-45\\9\\10\end{pmatrix}(\text{mod }26)$$

$$\begin{pmatrix}7\\9\\10\end{pmatrix}(\text{mod }26)$$

Hence the changing every value to the letter, the ciphertext message becomes

3	11	18	2	5	2	9	11	16	7	15	25	22	13	4	13	5	12
Z	H	O	Y	B	Y	F	H	M	D	L	V	S	J	A	J	B	I
21	17	0	12	22	8	4	7	17	20	17	8	7	9	10			
R	N	W	I	S	E	A	D	N	Q	N	E	D	F	G			

REFERENCES

1. **Advanced Encryption standard http:// csrc.nist. gov/encryption/aes/**
2. Data encryption standard (DES) ,Federal information processing Standards publication 46-3-1999
3. Oded Goldreich,Foundations of cryptography Volume – II Basic applications
4. Mark Stamp, Information Security principles and practice , 2002.
5. A.R. Vasishtha ,Modern Algebra, Krishna Prakashan Mandir, Meerut.
6. Advanced encryption standanred (AES) ,Federal information processing Standards publications ,197,2001
7. SergeLang,Introduction to linear algebra ,Second edition, springer
8. Oded Goldreich, Foundations of cryptography, volume I, Basic applications.
9. Dr. B.S. Grewal, Higher engineering mathematics, 40th edition, Khanna Publications.