

Encoding and Decoding

Cryptography :-

The study of coding & decoding a message is called as cryptography.
In the language of cryptography, the message to be sent is called as a plaintext;
Codes are called as ciphers & code messages are called as ciphertexts.

Enciphering (Encoding) :- The process of converting plain text by coding is called as a enciphering & the reverse process of getting plain text from the cipher text is called as a deciphering (decoding).

A selected matrix is called as a encoding matrix & its inverse is called as a decoding matrix.

Encoding matrix is called as a E-matrix.

General

Method:-

- 1:- To replace the words, ~~oblique~~ letters by nos.
- 2:- To encode the message.
- 3:- To decode the message.
- 4:- To replace nos by words/letters.

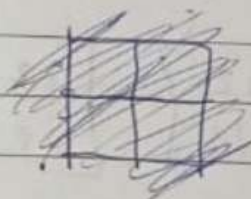
Note:- A goes to 1 Z goes to 26
B goes to 2

if the space betw 2 words goes to $X(27)$

A, B, C, ..., Z, X, * space } — (I)
 1 2 3 — — — 26, 27

Using a suitable 2×2 matrix encode & decode the message 'WEGO'
 23 5 7 15

To replace the words/letters by nos, from I we get the transformation

 W E G O
 23 5 7 15

We write this in a sequence of 2×1 matrix
 i.e. $\begin{bmatrix} 23 \\ 5 \end{bmatrix} \begin{bmatrix} 7 \\ 15 \end{bmatrix}$

To encode the message. We now pre-multiply each of the above column vectors by the encoding matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 5 \end{bmatrix} = \begin{bmatrix} 28 & 23 \\ 5 & 15 \end{bmatrix}$$

Columns of the above matrix gives the encoded message. The above message is transmitted in to the following linear form

28 5 23 15

S3

To decode the message
↳ The received message is now written
in a column matrix as

$$\begin{bmatrix} 28 & 22 \\ 5 & 15 \end{bmatrix}$$

The above matrix is then pre-multiplied
by the inverse of the coding matrix
i.e. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

$$\therefore \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 28 & 22 \\ 5 & 15 \end{bmatrix} = \begin{bmatrix} 23 & 7 \\ 5 & 15 \end{bmatrix}$$

S4 Replace nos by letters. the cols of
the above matrix in linear form as
23 5 7 15

When it is then it is transformed into
letters we get

23 5 7 15
W E H O

This is the original msg.

Q8 Using a suitable 2×2 encode & decode the
message 'NOW*STUDY'

In the previous eg. we did not consider the
space betn 2 words. Now But in this eg
we are considering the space betn 2 words
& assign the no. is 27.

For matrix multi. of size 2×2 , the last member of the Sec. should have 2 elements. Here we add space again after 'y' & consider the msg. as 'NOW STUDY'.

Step I :- ~~NO~~ Replace the words/letters by nos. 'NOW STUDY' from I we get the transformation

We write this in a sec-by 2×1 matrix.
i.e.
$$\begin{bmatrix} 14 \\ 15 \end{bmatrix} \begin{bmatrix} 23 \\ 27 \end{bmatrix} \begin{bmatrix} 19 \\ 20 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} \begin{bmatrix} 25 \\ 27 \end{bmatrix}$$

Step II :- To encode the message we pre multiply each of the above column vectors by the encoding matrix.
i.e. we get

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 14 & 23 & 19 & 21 & 25 & 27 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix} = \begin{bmatrix} 29 & 50 & 39 & 25 & 52 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

Step III :- To decode the message pre multiply by $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 29 & 50 & 39 & 25 & 52 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix} = \begin{bmatrix} 14 & 23 & 19 & 21 & 25 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

14 15 23 27 19 20 21 4 25 27
N O W S T U D Y