Deciphering/Decryption

The process of converting from cipher text to plain text is called deciphering.

The following example will explain the procedure for deciphering.

Example 6. Decipher the Cipher text = MOFZ for Key matrix = $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$.

Solution: Recall the formula which we used for enciphering

$$C = KP \pmod{26}$$

Formula for deciphering

$$P = K^{-1}C \pmod{26}$$

$$K^{-1} = \frac{Adj(A)}{\det(A)} \pmod{26}$$

Thus each plain text vector can be recovered from ciphertext vector by multiplying it on the left by $K^{-1} \pmod{26}$.

Step 1 First find K^{-1}, so det(K) = $|K| = \begin{vmatrix} 3 & 3 \\ 2 & 5 \end{vmatrix} = 15 - 6 = 9$

$$K^{-1} = \frac{\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}}{9} = 9^{-1}\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$$

What is the inverse of 9 modulo 26? Let it be x, then $9x = 1 \pmod{26}$

$$9.1 = 9 \neq 1 (\mathrm{mod} 26)$$

$$9.2 = 18 \neq 1 (\mathrm{mod} 26)$$

$$9.3 = 27 = 1 (\mathrm{mod} 26)$$

Hence, $9^{-1} = 3 \; (mod\ 26)$

Therefore,

$$K^{-1} = 9^{-1}\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = 3\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} (mod 26)$$

Step 2 Now, we will decipher MO first, then we will decipher FZ. For this we take

$$C = \begin{bmatrix} M \\ O \end{bmatrix} = \begin{bmatrix} 13 \\ 15 \end{bmatrix}$$

$$P = K^{-1}C \pmod{26} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 13 \\ 15 \end{bmatrix} = \begin{bmatrix} 450 \\ 395 \end{bmatrix} \pmod{26} = \begin{bmatrix} 8 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} H \\ E \end{bmatrix}$$

For FZ, $C = \begin{bmatrix} F \\ Z \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix}$

and P = $K^{-1}C$(mod 26)= $\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}\begin{bmatrix} 6 \\ 0 \end{bmatrix} = \begin{bmatrix} 90 \\ 120 \end{bmatrix}(mod\ 26) = \begin{bmatrix} 12 \\ 16 \end{bmatrix} \equiv \begin{bmatrix} L \\ P \end{bmatrix}$

So all plain text is HELP.

Example 7. Decode the following Hill 2-cipher, which was enciphered by the matrix A= $\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$

GTNKGKDUSK

Solution: We first find the inverse of A (mod 26) as

$$K^{-1} = 3^{-1}\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 9\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix}(mod 26) = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$$

Next we write numerical equivalent of cipher text, which is

7 20 14 11 7 11 4 21 19 11

To obtain the plaintext pairs, we multiply each ciphertext vector by the inverse of A (obtained in Example 6):

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 487 \\ 436 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix} \quad (\text{mod } 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 278 \\ 321 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix} \quad (\text{mod } 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 7 \\ 11 \end{bmatrix} = \begin{bmatrix} 271 \\ 265 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix} \quad (\text{mod } 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 4 \\ 21 \end{bmatrix} = \begin{bmatrix} 508 \\ 431 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} \quad (\text{mod } 26)$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}\begin{bmatrix} 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 283 \\ 361 \end{bmatrix} = \begin{bmatrix} 23 \\ 23 \end{bmatrix} \quad (\text{mod } 26)$$

From Table 1, the alphabet equivalents of these vectors are

ST RI KE NO WW

Which yields the message STRIKE NOW

Example 8 Decode 12 17 22 7 11 5

Using $A^{-1} = \begin{bmatrix} 1 & -6 & -8 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$

Solution:

Step 1
$$B = \begin{bmatrix} 12 & 7 \\ 17 & 11 \\ 22 & 5 \end{bmatrix}$$

$$A^{-1}B = \begin{bmatrix} 1 & -6 & -8 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 12 & 7 \\ 17 & 11 \\ 22 & 5 \end{bmatrix} = \begin{bmatrix} 20 & 5 \\ 9 & 21 \\ 13 & 16 \end{bmatrix}$$

That corresponds to $\begin{bmatrix} T & E \\ I & U \\ M & P \end{bmatrix}$ means Time up

EXAMPLE 5 A Number with No Reciprocal mod 26

The number 4 has no reciprocal modulo 26, because 4 and 26 have 2 as a common prime factor

For future reference, in Table 2 we provide the following reciprocals modulo 26:

Table 2 Reciprocals Modulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Work to do

Question 1. Determine whether the matrix is invertible modulo 26. If so, find its inverse modulo 26 and check your work by

$$AA^{-1} = A^{-1}A = I(mod\ 26)$$

a) $A = \begin{bmatrix} 9 & 1 \\ 7 & 2 \end{bmatrix}$ b) $B = \begin{bmatrix} 1 & 8 \\ 1 & 3 \end{bmatrix}$ c) $C = \begin{bmatrix} 2 & 1 \\ 1 & 7 \end{bmatrix}$

Question 2.

Decode the following Hill 2-cipher which was enciphered by the matrix $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

SAKNOXAOJX

Question 3.

Decode the Hill 3-cipher **XCVAFA** which was enciphered by the matrix key

$$\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 1 \end{bmatrix}$$