

Problem Statement:-

Consider the following stream cipher (which takes some ideas from the Enigma system used by Germans in World War II). Let π be a fixed permutation of Z_{26} and K a fixed element of Z_{26} . For all integers $i \geq 1$, the key stream element $Z_i \in Z_{26}$ is defined by

$$Z_i = (K + i - 1) \bmod 26.$$

Encryption and decryption using π are done as follows:

$$ez(x) = (\pi(x) + z) \bmod 26;$$

$$dz(y) = \pi^{-1}((y - z) \bmod 26);$$

Assuming

$$\pi \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 \\ 24 & 25 \end{pmatrix} = \begin{pmatrix} 23 & 13 & 24 & 0 & 7 & 15 & 14 & 6 & 25 & 16 & 22 & 1 & 19 & 18 & 5 & 11 & 17 & 2 & 21 & 12 & 20 \\ 4 & 10 & 9 & 3 & 8 \end{pmatrix}$$

Write a program to implement the cipher.

Input Specification:-

Plaintext or Cipher text, Key

Output Specification:-

Cipher text when Plain text is given as input and vice versa

Algorithm:-

Each letter from a to z refers to a corresponding index from 0 to 25 (letters are case insensitive). For our convenience we call them the corresponding letter indices in our algorithm. Also Z_i is calculated for a given key K .

Encryption:-

For a given string(plain text) every letter is encrypted as:
 $ez(x) = (\pi(x) + z) \bmod 26$ where x is the corresponding letter index for every letter in the given string. This encryption returns a letter index and this is converted to corresponding letter.

Decryption:-

For a given string(cipher text) every letter is decrypted as:
 $dz(y) = \pi^{-1}((y - z) \bmod 26)$ where y is the corresponding letter index for every letter in the given string. This decryption returns a letter index and this is converted to corresponding letter.

Sample Input:-

Encryption:-

1)

Key: 12

Plain text: hello

2)

Key: 25

Plain text: WORLD

Decryption:-

1)

Key:13

Cipher text: Wupnvkz

2)

Key: 1

Cipher text: nEj

Output of Sample Input:

Encryption:-

1)rtopu

2)IECCC

Decryption:-

1) Welcome

2) bYe