**Bifid Decrypt Solution**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Column** | | | | | |
| **0** | **1** | **2** | **3** | **4** | **5** |
| **Row** | **0** | “B” | “G” | “0” | “W” | “K” | “Z” |
| **1** | “Q” | “1” | “P” | “L” | “D” | “S” |
| **2** | “9” | “I” | “0” | “X” | “7” | “E” |
| **3** | “F” | “4” | “C” | “U” | “M” | “6” |
| **4** | “T” | “H” | “2” | “V” | “R” | “5” |
| **5** | “N” | “A” | “8” | “Y” | “3” | “J” |

Ciphertext: “21IYC”

First, we will create 2 dictionaries using the matrix.

characterDict = {character : (row,column)}

positionDict = {(row,column) : character}

This is so that each time we decode a character in the ciphertext, we don’t have to search through the entire matrix to find the corresponding (row,column) and vice versa.

Then, we can loop through the ciphertext “21IYC?” and append the row and column of each character to an array using the characterDict which will result in the following:  
characterArray = [4, 2, 1, 1, 2, 1, 5, 3, 3, 2] --> [ 2 = (4,2); 1 = (1,1); I = (2,1); Y = (5,3); C = (3,2) ]

Now, since we are reversing the bifid encryption, each plaintext character's rows are in the first half of the character array and the columns are in the second half. It can be thought of as follows:

characterArrayRow = [4,2,1,1,2] [1,5,3,3,2] = characterArrayColumn

Thus, we can loop through the ciphertext, and if the character is in the matrix, we can append the corresponding character in the matrix with the row from the first half of characterArray and the column from the second half of characterArray.

We will initialize an index counter at 0 and loop through the ciphertext. If the character is in the matrix, then we’ll look in the positionDict for (index counter, index counter + length(characterArray)//2) and append the corresponding character to the plaintext and then add 1 to the index counter. Otherwise, we can just append the character to the plaintext because it’ll be a special character.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Cipher Character** | 2 | 1 | I | Y | C | ? |
| **Row** | 4 | 2 | 1 | 1 | 2 |  |
| **Column** | 1 | 5 | 3 | 3 | 2 |  |
| **Plaintext Character** | H | E | L | L | O | ? |

The returned string is the resulting plaintext “HELLO?”.