A Friendly Competition - Part 2

Problem Submissions Leaderboard Discussions

You and your best friend Dhruvi have taken the Cryptography course in your respective colleges. Dhruvi often boasts about being smarter than you. One day when you were discussing Cryptography and puzzles, a heated debate starts between the two of you regarding who is better at solving puzzles. To settle this debate you guys decide to come up with a cipher each. You both agree to text via WhatsApp using the ciphertext generated by your ciphers, which means that Dhruvi will send you her message as the ciphertext generated by her cipher and you'll respond by sending your message as the ciphertext generated by your cipher. The challenge is that you will have 10 seconds to respond to each others' messages. Whomsoever fails to do so first loses the challenge.

Your cipher:

To prove that you are better than Dhruvi, you decide to dive deep into the pre-existing ciphers and upon doing so you find a lot of interesting ciphers. Acknowledging the fact that Dhruvi isn't just "all talk and no brains", you decide to take things up a notch by double encrypting your message using a primary cipher that is new to both of you. Taking inspiration from the recently learned different variations of DES algorithm, you decide to implement a Rail fence transposition on the output from a partially implemented Straddle Checkerboard cipher.

The Encryption algorithm:

This algorithm is a product cipher of two ciphers: Straddle Checkerboard and Rail fence Transposition. The encrypting takes place in two phases. First phase is performing substitution while the second phase is transposition.

1. During the substitution phase, we substitute each letter with either one or more digits retrieved from the straddle checkerboard (https://en.m.wikipedia.org/wiki/Straddling_checkerboard)
2. After this, impose rail fence transposition on the output of the straddle checkerboard. (https://privacycanada.net/rail-fence-cipher/)

Refer to the following link for a detailed explanation with example: http://practicalcryptography.com/ciphers/straddle-checkerboard-cipher/

NOTE:

- Remember we stop the algorithm after encoding it with the initial matrix setup. We **DO NOT** proceed to add a new secrect key number **nor do we convert** the cipher numbers to letters again using the same setup during encryption.
- Please keep in mind that the above algorithm is that of Encryption whereas you are asked to write the code for ***Decryption*** of this particular algorithm.

Input Format

The input consists of 4 lines where:

1. The first line consists of the "key" for straddling checkerboard
2. The second line consists of digits excluded from the first row of the straddle checkerboard
3. The third line consists of the ciphertext to decrypt

4. The fourth line consists of an integer which will be the “Key” (denoting the number of rows to be used) for the rail fence transposition.

Constraints

The ciphertext to decrypt consists of a permutation of the digits [0-9] only.

Output Format

Plain text – String

Sample Input 0

```
XZDECAMRQKUYBLFOGVITWJHPSN
2 7
377767272277661122967521077712672277
3
```

Sample Output 0

```
DONTASKTAFORSOLUTION
```

Explanation 0

Note: Remember we stop the algorithm after encoding it with the initial matrix setup. We **DO NOT** proceed to add a new secrect key number **nor do we convert** the cipher numbers to letters again using the same setup during encryption.

Contest ends in an hour

Submissions: 164
Max Score: 6
Difficulty: Medium

Rate This Challenge:
☆ ☆ ☆ ☆ ☆

More

C++20

```
#include <cmath>
#include <cstdio>
#include <vector>
#include <iostream>
#include <algorithm>
using namespace std;


int main() {
    /* Enter your code here. Read input from STDIN. Print output to STDOUT */
    return 0;
}

```

Line: 1 Col: 1

Upload Code as File   □ Test against custom input   Run Code   Submit Code