A Friendly Competition - Part 1

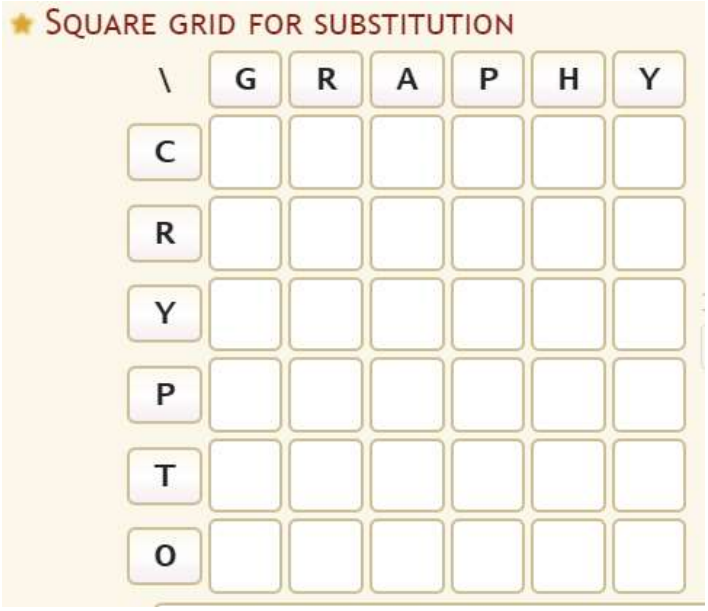
You and your best friend Dhruvi have taken the Cryptography course in your respective colleges. Dhruvi often boasts about being smarter than you. One day when you were discussing Cryptography and puzzles, a heated debate starts between the two of you regarding who is better at solving puzzles. To settle 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 will 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.

Dhruvi's Cipher:

Conservative in her thought process, Dhruvi decides to teach you a lesson and since you hate history, she goes to ChatGPT and asks about ciphers used in the World War. To her surprise she gets a lot of good ciphers that can be difficult to solve in the short amount of time you have agreed to. The following excerpt catches her eye:

*"In cryptography, the **ADFGVX cipher** was a manually applied field cipher used by the Imperial German Army during World War I. It was used to transmit messages secretly using wireless telegraphy. ADFGVX was in fact an extension of an earlier cipher called ADFGX which was first used on 1 March 1918 on the German Western Front. ADFGVX was applied from 1 June 1918 on both the Western Front and Eastern Front."*

She very well knows that you are quite good at solving standard puzzles so she decides to throw a curveball at you by modifying the standard ADFGVX cipher. She adds an extra layer to the pre-existing algorithm, instead of naming the rows with the letters ADFGVX, she names them CRYPTO and the columns as GRAPHY. (as shown below)



Given a key square (polybius square), keyword and plaintext message, encrypt the message using the modified ADFGVX cipher and return the cipher text.

About the algorithm:

This algorithm is a product cipher of two ciphers: polybius square cipher and columnar transposition. The encrypting takes place in two phases. First phase is performing substitution while the second phase is fractionating.

1. During the substitution phase, we substitute each letter with two letters retrieved from the polybius square (https://en.wikipedia.org/wiki/Polybius_square)
2. After this, fill the enciphered text below the keyword in a matrix format left to right in a row and top to bottom fashion. Now perform columnar transposition by sorting the keyword in alphabetical order. (https://privacycanada.net/columnar-transposition-cipher/)
3. Now retrieve the text from the matrix column wise top to down to get the final ciphered text. Refer to the following link for a detailed explanation with example: http://practicalcryptography.com/ciphers/classical-era/adfgvx/

Input Format

The input consists of 3 lines where:

1. The first line consists of the keyword for columnar transposition
2. The second line consists of a permutation of the alphabets (in upper case) and digits. This should be used to fill the polybius square in left to right fashion
3. The third line consists of the plain text to encrypt

Constraints

- The input string will consist of A-Z characters i.e.., English alphabets in upper case and 0-9 digits only. (Total 36 characters in the Polybius Square key)
- You have to **fill the empty spaces** in the matrix during the columnar transposition step **using the character 'X'**. Which means that your cipher text may contain the character 'X' along with a certain permutation of the characters of the word 'CRYPTOGRAPHY'.

Output Format

Cipher text – String

Sample Input 0

```
CIPHER
J9I1E8D2Z6Y3M0C7K5LQOX4SFTUAGHNRWPBV
TEXTTOENCRYPT
```

Sample Output 0

```
TTCOTPPYOXHRGHXRRHRRCTORXPAAPX
```

Explanation 0

You have to **fill the empty spaces** in the matrix during the columnar transposition step **using the character 'X'**. Which means that your cipher text may contain the character 'X' along with a certain permutation of the characters of the word 'CRYPTOGRAPHY'.