A Cryptic Connection

In the enthralling landscape of a cryptography competition, where intellectual curiosity permeated the air and the buzz of innovation filled every corner, an eagerly anticipated annual cryptography competition event dominated conversations. As the competition drew near, whispers circulated about a mysterious algorithm, adding an extra layer of intrigue to the upcoming challenge. Rumors hinted at the creation of an enigmatic contributor that had piqued the curiosity of all participants.

Amidst the anticipation and excitement, you, a budding cryptography enthusiast, found yourself captivated by the allure of the challenge. The rumor mill hinted that the mind behind this cryptic creation was none other than your mysterious crush.

With the competition drawing near, the cryptic algorithm was revealed, leaving participants scratching their heads in bewilderment. The challenge was clear: decrypt the algorithm to unravel the hidden message within. Determined to seize the opportunity and impress not only the cryptography community but also your crush, you embarked on a journey to decipher the intricate layers of this amalgamation of three different ciphers.

Little did you know that the pursuit of unraveling the cryptographic enigma would lead you to unexpected twists, intricate patterns, and perhaps, a deeper connection with the mysterious mind behind the challenge. The atmosphere of the competition echoed with whispers of anticipation, and the challenge stood as a testament to the cryptic connection that transcended the boundaries of individual participants, bringing together brilliant minds from different corners of the cryptic community.

About the algorithm:

The given algorithm is a product cipher, combining the strengths of Playfair, Vigenère, and Columnar Transposition ciphers to enhance the security of the encryption process.

1. Playfair cipher: Employing the Playfair cipher involves the generation of a key table derived from a given keyword. The plaintext is then broken into digraphs, pairs of letters, and each digraph undergoes the Playfair encryption process. This step serves as the initial layer in our product cipher, introducing a spatial transformation to the original message.

2. Vigenère Cipher: The Vigenère cipher introduces an additional layer of complexity. Utilizing a chosen keyword, it is repeated to match the length of the plaintext. The combination of this extended keyword and the original plaintext occurs through the Vigenère square, resulting in a transformed ciphertext. This second layer adds a dynamic element to our cryptographic puzzle.

3. Columnar Transposition Cipher: The third and final layer involves the Columnar Transposition cipher. The Vigenère ciphertext is systematically rearranged into a grid, adhering to a specified columnar transposition key. Reading the columns of this grid in the order dictated by the key produces the ultimate ciphertext. This sequential application of ciphers in a product fashion contributes to the overall robustness of our cryptographic algorithm.

4. Please refer to the following three links for a detailed explanation with examples for the specified algorithms:
   - Playfair cipher: https://privacycanada.net/playfair-cipher/
   - Vigenère Cipher: https://privacycanada.net/classical-encryption/vigenere-cipher/
   - Columnar Transposition Cipher: https://privacycanada.net/columnar-transposition-cipher/

NOTE:

- In the Playfair cipher, the convention we follow here is to exclude 'I' and 'J' from sharing the same cell, and 'J' is removed from the matrix.

- For the columnar transposition cipher during encryption, if the last row has empty cells, they should be filled with the character 'X'.
- It's important to note that the decryption process for these adjustments will need to be considered and implemented accordingly.

Input Format

The input consists of 4 lines where:

1. The first line contains the key for the Playfair cipher.
2. The second line contains the key for the Vigenere cipher.
3. The third line contains the key for the Columnar Transposition cipher.
4. The fourth line contains the ciphertext to be decrypted.

Constraints

- It is to be assumed that in the outputs generated by the Playfair and Vigenère ciphers, none will contain the alphabet 'X'. Therefore, the presence of 'X' in the final ciphertext can be attributed solely to the application of the columnar transposition cipher.
- The input strings will pertain to the language {A-Z}.
- You are not allowed to use libraries like cryptography available in python.

Output Format

Print the plaintext in uppercase string format.

Sample Input 0

```
TRICIPHER
CODEHELP
FINAL
GXTWVSYXQP
```

Sample Output 0

```
TESTCODE
```

Contest ends in an hour

Submissions: 137
Max Score: 7
Difficulty: Hard

Rate This Challenge:
☆☆☆☆☆

More

C++20

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

```