Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the Vigenère square or Vigenère table.

The table consists of the alphabets written out 26 times in different rows, each alphabet shifted ***cyclically to the left compared to the previous alphabet***, corresponding to the 26 possible Caesar Ciphers.

At different points in the encryption process, ***the cipher uses a different alphabet from one of the rows***.

The alphabet used at each point depends on a repeating keyword.

Example:

Input : Plaintext : GEEKSFORGEEKS

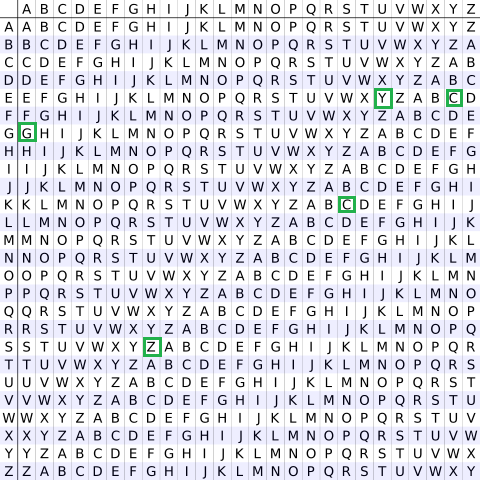
Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

The plain text is then encrypted using the process explained below.



#### Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

Decryption  
Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column’s label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

An easier **implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

**Encryption**

The the plaintext(P) and key(K) are added modulo 26.

Ei = (Pi + Ki) mod 26

**Decryption**

Di = (Ei - Ki + 26) mod 26

**Note:** Di denotes the offset of the i-th character of the plaintext. Like offset of **A** is 0 and of **B** is 1 and so on.

1. Given the above description of the Vigenère cipher, create a C++ program that **encrypt and decrypts a message from the user**.
2. Test the program to verify that the output is accurate. Assess program limitations.
3. Provide documentation that entails programming approach for encryption and decryption.

