10802 CPP Midterm Exam

Contributor：Pin-Shao Chen

Subject：Playfair Cipher

Main testing concept：

Basics	Functions
■ C++ BASICS	□ SEPARATE COMPILATION AND NAMESPACES
□ FLOW OF CONTROL	□ STREAMS AND FILE I/O
■ FUNCTION BASICS	□ RECURSION
□ PARAMETERS AND OVERLOADING	□ INHERITANCE
■ ARRAYS	□ POLYMORPHISM AND VIRTUAL FUNCTIONS
□ STRUCTURES AND CLASSES	□ TEMPLATES
□ CONSTRUCTORS AND OTHER TOOLS	□ LINKED DATA STRUCTURES
□ OPERATOR OVERLOADING, FRIENDS, AND REFERENCES	□ EXCEPTION HANDLING
■ STRINGS	■ STANDARD TEMPLATE LIBRARY
□ POINTERS AND DYNAMIC ARRAYS	□ PATTERNS AND UML

Description：

The Playfair cipher is a manual symmetric encryption technique. The principle of this technique is to create a 5*5 key-value table based on a given word, which is used to encrypt the plaintext in accordance with certain rules.

Please write a program to encrypt the plaintext using the Playfair cipher which should satisfy following requirements.

1. **Key table generation**

   First fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order, and put both "I" and "J" in the same space. (You can simply regard "J" as "I".)

   Example:
   Keyword(key) : **PLAYFAIREXAMPLE**

P	**L**	**A**	**Y**	**F**
I/J	**R**	**E**	**X**	**M**

   First, put the letters of the keyword in the top rows of the table, from left to right, and dropping any duplicate letters.

P	**L**	**A**	**Y**	**F**

I/J	**R**	**E**	**X**	**M**
B	**C**	**D**	**G**	**H**
K	**N**	**O**	**Q**	**S**
T	**U**	**V**	**W**	**Z**

Then fill the remaining spaces with the rest of the letters of the alphabet in order.

2. **Pre-process the message**

To encrypt a message, the algorithm should first break the message into groups(each contains 2 letters) such that, "**HelloWorld**" becomes "**HE LL OW OR LD**".

- If **both letters** in a group are **the same,** the algorithm should add an "**X**" after the first letter, while pushing the second letter backward.
  For example, "**HE LL OW OR LD**" should be processed to become "**HE LX LO WO RL D** ".
- If there is **only one letter** in a group, the algorithm should add an "**X**" at the end.
  For example, "**HE LX LO WO RL D**" should be processed to be "**HE LX LO WO RL DX**".

3. **Encryption**

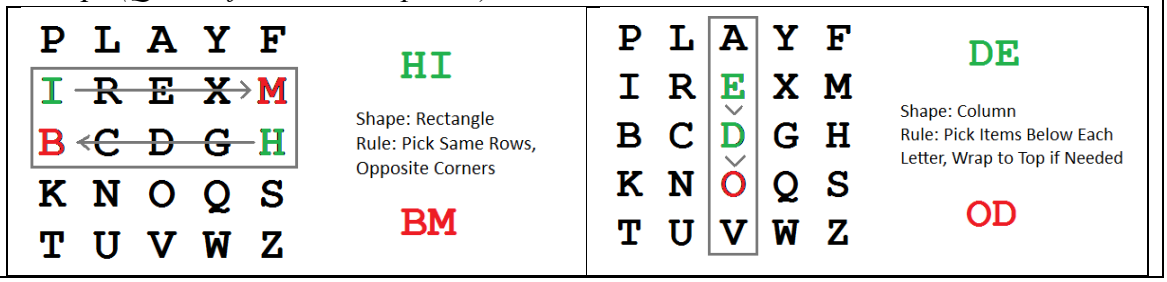
Encryption will be performed using the set of groups obtained in step 2.
For each set (letter1, letter2), find the position of each letter in the table then encrypt them by the rules descript below:

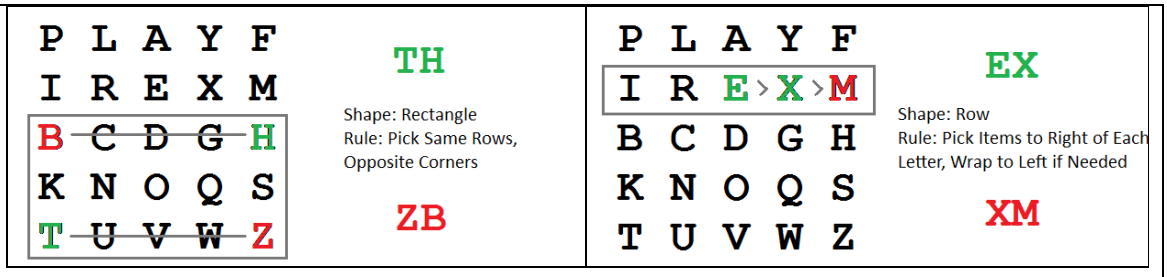
A. If the two letters of the set are in the same **column** of the key table:
   Get the encrypted letters from the key table by the down one of each letter. Upon reaching end of table, wrap around.

B. If the two letters of the set are in the same **row** of the key table:
   Get the encrypted letters from the key table by the right one of each letter. Upon reaching end of table, wrap around.

C. If the two letters of the set are in the same **rectangle** of the key table:
   Get the encrypted letters from the key table by swapping the letters with the ones on the end of the rectangle..

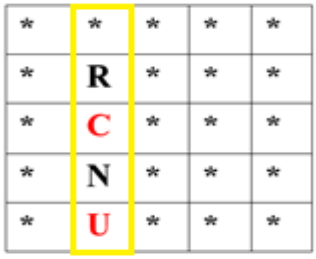
Example*(Quoted from the Wikipedia.)*:





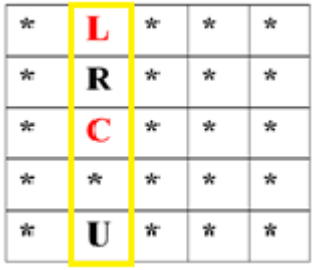
More encrypting examples:

For the pair of letters "**RN**", we can get the new encoded text "**CU**" by following rule 1.



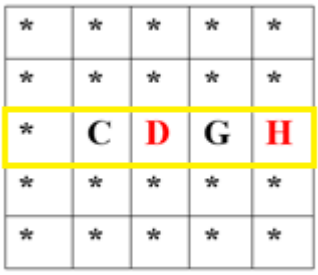
RN=>CU

For the pair of letters "**UR**", we can get the new encoded text "**LC**" by following rule 1.



UR=> LC

For the pair of letters "**CG**", we can get the new encoded text "**DH**" by following rule 2.



CG => DH

For the pair of letters "**YF**", we can get the new encoded text "**FP**" by following rule 2.

YF => FP

For the pair of letters "**HE**", we can get the new encoded text "**DM**" by following rule 3.

HE => DM

For the pair of letters “**LO**”, we can get the new encoded text “**AN**” by following rule 3.

LO => AN

Input：

Every two lines is a test set, the first line is the **plaintext** and the second line is the **keyword,** please encrypt the given **plaintext** using Playfair cipher.

** The plaintext **will not** contain repeat ‘X’ letters or be end with an ‘X’ letter.
** The given **plaintext** and **keyword** would all be lowercase letters, you don't need to check that the input format is correct.

Output：

Output the text encrypted by Playfair Cipher with the given **plaintext** and **keyword**.

Sample Input / Output :

Sample Input	Sample Output
helloworld playfairexample	dmyranvqcrge
ntustcsie objectorientedprogramming hidethegoldinthetreestump playfairexample	drkupoqeiy bmodzbxdnabekudmuixmmouvif
…	…

□ **Easy, only basic programming syntax and structure are required.**

□ **Medium, multiple programming grammars and structures are required.**

■ **Hard, need to use multiple program structures or complex data types.**

Expected solving time:

40 minutes

Other notes: