

**DWITE Online Computer Programming Contest
December 2006**

Problem 5

Caesar's Cipher

In cryptography, a Caesar's cipher is one of the simplest and most widely-known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on, X would become A, Y would become B and Z would become C.

The Caesar cipher can be easily broken if the decipherer knows that a Caesar cipher is in use and knows the shift value.

The input file (**DATA51.txt** for the first submission and **DATA52.txt** for the second submission) will contain five sets of data. Each set will contain two lines. The first line will contain a message that was encrypted using the Caesar Cipher. The line will contain no more than 255 characters and the characters will be upper case. The second line will contain the decrypted first word of the encrypted message.

The output file (**OUT51.txt** for the first submission and **OUT52.txt** for the second submission) will contain five lines of data, corresponding to each line of the input file. Each line of data will contain the decrypted message.

Sample Input (Only three sets of data given)

```
KHOOR GZLWH.  
HELLO  
JKIKSHKX OY BKXXXXXXXXE IURJ....  
DECEMBER  
CAH RC. HXD'UU URTN RC.  
TRY
```

Sample Output (Only three lines given)

```
HELLO DWITE.  
DECEMBER IS VERRRRRRY COLD....  
TRY IT. YOU'LL LIKE IT.
```

To learn more about the Caesar Cipher, visit http://en.wikipedia.org/wiki/Caesar_cipher