1687 - Vigenere Cipher Encryption

Description

One of the oldest and most common encryption algorithms is Vigenere Cipher. It is quite an old thing? A similar encryption was first described in 1553 by Giovan Battista Bellaso and improved in 1586 by Blaise de Vigenere.
Vigenere encryption produces a single letter of ciphertext for each letter of plaintext, combining one plaintext letter with one single letter of a key on the corresponding position. If the key is shorter than the plaintext, it is simply repeated as needed, e.g. for a key of length 3 and plaintext of length 7, letters will be combined like this (Ki is the key letter, Pi is the plaintext letter, and Ci is the resulting ciphertext letter).

K1	K2	K3	K1	K2	K3	K1
P1	P2	P3	P4	P5	P6	P7
C1	C2	C3	C4	C5	C6	C7

The letter of the key specifies how many positions should be the plaintext letter "shifted forward" in the alphabet. If a key letter is A, the correspoding plaintext letter will be shifted by one character, B means two positions, etc. The alphabet is considered circular, so if the last letter (Z) should be shifted, it becomes A again. Please note that A (key) combined with another A (plaintext) will result in B, which may be a little unusual for the common Vigenere cipher. The Vigenere square at the end of this problem statement gives an overview how letters of a plaintext get combined with letters of a key to produce the ciphertext.

Your task is to write a program that will encrypt messages using the Vigenere cipher with a given key.

Input specification

The input contains several instances. Each instance consists of two lines, the first line is the encryption key and the second line is the plaintext. Both key and plaintext consist of uppercase letters of the English alphabet {A, B, C, ..., Z}. The length of the key will be between 1 and 1000, the length of the plaintext between 1 and 100000, inclusive. Input is terminated by a line containing one zero.

Output specification

For each input instance, output the ciphertext - the encrypted version of the message.

Sample input

```
ICPC
THISISSECRETMESSAGE
ACM
CENTRALEUROPEPROGRAMMINGCONTEST
LONGKEY
CERC
0
```

Sample output

```
CKYVRVIHLUUWVHIVJJU
DHAUUNMHHSRCFSEPJEBPZJQTDRAUHFU
OTFJ
```

Hint(s)

* A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Source	2010/2011 ACM-ICPC Central Europe Regional Contest
Added by	**ymondelo20**
Addition date	2012-02-18
Time limit (ms)	2000
Test limit (ms)	2000
Memory limit (kb)	150000
Output limit (mb)	64
Size limit (bytes)	30000
Enabled languages	C C# C++ Java Pascal Perl PHP Python Ruby Text