For many centuries, most — if not all — known methods for enciphering messages considered a single cipher alphabet. For example, Julius Caesar used a substitution cipher that replaced each letter in the plaintext message by a letter three places further down in the alphabet ('A' would be 'D' and so on).

Sometime in the 16th century, a French diplomat called Blaise de Vigenère perfected a new cipher based on previous work by Leon Alberti, Johannes Trithemius and Giovanni Porta. The most significant breakthrough was the use of multiple cipher alphabets, which turned the cipher impregnable to frequency analysis (a technique for deducing the plaintext from a ciphertext).

## How to encipher a plaintext message

The first step in encipherment is to draw a Vigenère square:

```
PLAINTEXT LETTERS
```

labcdefghijklmnopqrstuvwxyz

```
(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
   1
       (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
   2
       (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
   3
   4
       (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
   5
       (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) \hspace{0.1cm} | \hspace{0.1cm} G \hspace{0.1cm} H \hspace{0.1cm} I \hspace{0.1cm} J \hspace{0.1cm} K \hspace{0.1cm} L \hspace{0.1cm} M \hspace{0.1cm} N \hspace{0.1cm} O \hspace{0.1cm} P \hspace{0.1cm} Q \hspace{0.1cm} R \hspace{0.1cm} S \hspace{0.1cm} T \hspace{0.1cm} U \hspace{0.1cm} V \hspace{0.1cm} W \hspace{0.1cm} X \hspace{0.1cm} Y \hspace{0.1cm} Z \hspace{0.1cm} A \hspace{0.1cm} B \hspace{0.1cm} C \hspace{0.1cm} D \hspace{0.1cm} E \hspace{0.1cm} F
C
   6
       (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
Ι
   7
       (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
Ρ
   8
      (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
Η
   10 (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
Ε
   11 (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
   12 (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
Α
   13 (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
   14 (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
L
Ρ
   15 (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
   16 (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
Η
   17 (Q) | RSTUVWXYZABCDEFGHIJKLMNOPQ
Α
   18 (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
В
   19 (S) | TUVWXYZABCDEFGHIJKLMNOPQRS
Ε
Τ
   20 (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
   21 (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
   22 (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
   23 (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
   24 (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
   25 (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
   26 (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
```

must be chosen. A practical way of doing this is via a keyword. For example, the keyword 'MIUP' selects the cipher alphabets 13, 9, 21 and 16 (see underlined rows in the Vigenère square). In the final step, each letter in the plaintext message is enciphered according to the corresponding

Then, the multiple cipher alphabets (rows in the Vigenère square) to be used in the encipherment

cipher alphabet. For example, suppose the plaintext message is 'programming' and the keyword is 'MIUP.' The encoded message would be: i n g M I U

```
cipher alphabets - 13 9 21 16 13 9 21 16 13 9
encoded message \, - \, C \, A \, J \, W \, E \, J \, H \, C \, V \, W \, B
  The letter 'p' in the plaintext message is enciphered using cipher alphabet 13 into the letter 'C'.
```

The 'C' comes from the intersection of column 'p' with row 13 in the Vigenère square. The second letter in the plaintext message, 'r', is enciphered into the letter 'A' using cipher alphabet 9 (check the intersection of column 'r' with row 9), and so on. If necessary, as in this case, the keyword can be repeated multiple times to match the length of the plaintext message. How to decipher an encoded message

The decipherment of an encoded message requires the keyword that was used to encipher the

M I

# plaintext message. For example, suppose the encoded message is 'CAJWEJHCVWB' and the keyword

is 'MIUP'. H C encoded message - C A J W Ε

```
plaintext message - p r o g r a m m
   The multiple cipher alphabets of 'MIUP' are, again, 13, 9, 21 and 16 (grey rows in the Vigenère
square above). Each plaintext message letter is obtained by finding the corresponding encoded letter in
the row of the current cipher alphabet and then checking the letter on top of the column. For example,
```

cipher alphabets - 13 9 21 16 13 9 21 16 13 9 21

- M I U P M I U P

the letter 'p' in the plaintext message is on top of the column where 'C' (the encoded letter) appears in row (cipher alphabet) 13. The decipherment ends when the last encoded letter is deciphered. (This background was written based on Simon Singh's "The Code Book," p. 45-51.) Input

The input will consist of multiple lines. Each line contains a message enciphered with the Vigenère cipher (in uppercase). The only knowl-

## edge about each message is that after being deciphered it represents a 3 digit number written as text (for example: 'oneoneone' or 'zerozeroseven').

message.

Output

Separate the output of each input line with a single blank line. For each line, the output is all possible decipherments of the encoded message. For example, the encoded message 'PQRPQRPQR' means 'oneoneone' when the keyword is 'ACM', but also means

'oneonetwo' or 'oneonesix' when the keywords are, respectively, 'ACMACMVTC' and 'ACMACMWHT', and so

Each decipherment is written in a single line, as shown in the sample output. The text to the left of the '->' symbol is the keyword (in uppercase) and to the right is the corresponding plaintext 3 digit number (in lowercase). There should be no empty line between decipherments of the same input

Note: the output must be sorted in descending order by value of the plaintext number ('nineninenine'  $\ensuremath{\upolesise{\oolesi$ Sample Input

PQRPQRPQR Sample Output

### WHTWHTWHT -> sixsixsix WHTWHTVTC -> sixsixtwo

WHTWHTACM -> sixsixone WHTVTCWHT -> sixtwosix WHTVTCVTC -> sixtwotwo

**PQRPQRPQR** 

#### WHTVTCACM -> sixtwoone WHTACMWHT -> sixonesix WHTACMVTC -> sixonetwo

WHTACMACM -> sixoneone

VTCWHTWHT -> twosixsix VTCWHTVTC -> twosixtwo VTCWHTACM -> twosixone VTCVTCWHT -> twotwosix VTCVTCVTC -> twotwotwo VTCVTCACM -> twotwoone VTCACMWHT -> twoonesix VTCACMVTC -> twoonetwo VTCACMACM -> twooneone ACMWHTWHT -> onesixsix ACMWHTVTC -> onesixtwo ACMWHTACM -> onesixone ACMVTCWHT -> onetwosix ACMVTCVTC -> onetwotwo ACMVTCACM -> onetwoone ACMACMWHT -> oneonesix ACMACMVTC -> oneonetwo ACMACMACM -> oneoneone WHTWHTWHT -> sixsixsix WHTWHTVTC -> sixsixtwo WHTWHTACM -> sixsixone WHTVTCWHT -> sixtwosix WHTVTCVTC -> sixtwotwo

WHTACMACM -> sixoneone VTCWHTWHT -> twosixsix VTCWHTVTC -> twosixtwo

WHTVTCACM -> sixtwoone WHTACMWHT -> sixonesix WHTACMVTC -> sixonetwo

VTCWHTACM -> twosixone VTCVTCWHT -> twotwosix VTCVTCVTC -> twotwotwo

VTCVTCACM -> twotwoone VTCACMWHT -> twoonesix VTCACMVTC -> twoonetwo VTCACMACM -> twooneone

ACMWHTWHT -> onesixsix ACMWHTVTC -> onesixtwo ACMWHTACM -> onesixone ACMVTCWHT -> onetwosix

ACMVTCVTC -> onetwotwo

ACMVTCACM -> onetwoone ACMACMWHT -> oneonesix ACMACMVTC -> oneonetwo ACMACMACM -> oneoneone