> For many centuries, most - if not all - known methods for enciphering messages considered a sin
> $\begin{aligned} & \text { For many centuries, most - if not all - known methods for enciphering messages considered a single } \\ & \text { cipher alphabet. For example, Julius Caesar used a substitution cipher that replaced each letter in th. } \\ & \text { plaintext message by a letter three places further down in the alphabet ' } A \text { ' would be ' } D \text { ' and so on). }\end{aligned}$ $\begin{aligned} & \text { plaintext message by a letter three places further down in the alphabet ' ' } A \text { ' would be ' } D \text { ' and so on). } \\ & \text { Sometime in the 16th century, a French diplomat called Blaise de Vigenere perfected a new ciphe }\end{aligned}$ $\begin{aligned} & \text { Sometime in the 16th century, a French diplomat called Blaise de Vigenère perfected a new cipher } \\ & \text { based on previous work by Leon Alberti, Johannes Trithemius and Giovanni Porta. The most significant }\end{aligned}$ $\begin{aligned} & \text { breakthrough was the use of multiple cipher alphabets, which turned the cipher impregnable to frequency } \\ & \text { nalysis (a technique for deducing the plaintext from a ciphertext). }\end{aligned}$ $\begin{aligned} & \text { analysis (a technique for deducing the plainte } \\ & \text { How to encipher a plaintext message } \\ & \text { The first step in encipherment is to draw }\end{aligned}$
> The first step in encipherment is to draw a Vigenère square:

Then, the multiple cipher alphabets (rows in the Vigenère square) to be used in the enciphermen
nust 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 Vigesenere square).
In the final step, each letter in the plaintext message is enciphered according to te In the final step, each cipher alphabet. For example, suppose
MIUP. 'The encoded message would be:

encoded message - C A J W E J H C V W
The letter ' p ' in the plaintext message is enciphered using cipher alphabet 13 into the letter ' $c$. he ' C ' comes from the intersection of column ' p ' with row 13 in the Vigenère square. The second
的

How to decipher an encoded message
The decipherment of an encoded message requires the keyword that was used to encipher the
plaintext message. For example, suppose the encoded message is 'CAJWEJHCVWB' and the keyword plaintext
is 'IIUP'
$\begin{array}{llllllllllllll}\text { encoded message } & - & \text { C } & \text { A } & \text { J } & \text { W } & \text { E } & \text { J } & \text { H } & \text { C } & \text { V } & \text { W } & \text { B } \\ \text { keyword } \\ \text { cipher alphabets } & - & \text { M } & \text { I } & \text { U } & \text { P } & \text { M } & \text { I } & \text { U } & \text { P } & \text { M } & \text { I } & \text { U } \\ \text { c } & 21 & 216 & 13 & 9 & 21 & 16 & 13 & 9 & 21\end{array}$

The multiple cipher alphabets of 'MIUP' are, again, $13,9,21$ and 16 (grey rows in the Vigenère
uare above). Each plaintext message letter is obtained by finding the corresponding encoded letter in square above). Each plaintext message letter is obtained by finding the corresponding encoded letter in
he row of the current cipher alphabet and then checking the letter on top of the column. For example the letter 'p' in the plaintext message is on top of the column where 'c' '(the encoded letter) appe (cipher alphabet) 13. The decipherment ends when the last encoded letter is deciph)
(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 contais a muss
le he contains a message enciphered with the Vigenère cipher (in uppercase). The only knowl. (for example: 'oneoneone' or 'zerozeroseven')

Output
Separate the output of each input line with a single blank line.
For each line, the output is all possible decipherents of the encoded message. For example ench 'ach ine, the output is all possible decipherments of the encoded message. For example, oneonetwo' or 'oneonesix' when the keywords are, respectively, 'ACMACMVTC' and 'ACMACMMHT', and so Each decipherment is written in a single line, as shown in the sample output. The text to the
left of the ' $\rightarrow$ ’ symbol is the keyword (in uppercase) and to the right is the corresponding plaintext 3 left of the 's-> 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 message.
Note: the output must be sorted in descending order by value of the plaintext number ('nineninenine'
'ninenineeight'
PQRPQRPQR
PQRPQRPQR
Sample Output

| ПнтинтинT |  |
| :---: | :---: |
| wHTWHTVTC | sixsixtwo |
| wHTwHTACM |  |
| whtvicwht | sixtwosix |
| whtvicvic | sixt |
| whTvTCACM | sixtwoone |
| whTacmuht | sixonesix |
| whTacmvic | sixonetwo |
| whTacmacm | sixoneone |
| vтСинтWHT | twosixsix |
| vTCwHTVTC | twosixtwo |
| vтсинTACM | twosixone |
| vtcvicwht | twotwosix |
| vTCvTCVTC | twotwotwo |
| vtcvicacm | twotwoone |
| vTCACMWHT | twoonesix |
| vtcacmvic | twoonetwo |
| vtcacmacm | twooneone |
| ACMnHTHHT | onesixsix |
| ACMWHTVTC | onesi |
| АСММНTTACM | onesixone |
| ACMvTCWHT | onetwosix |
| ACMvTCVTC | onetwotwo |
| ACMVTCACM | e |
| ACMACMVHT | oneone |
| acmacmvic | one |
| ACMACMACM | oneoneone |
| wh |  |
| wHTwHTVTC | si |
| whTwhtacm | six |
| whtvichit | sixtwo |
| whtvicvic | si |
| whtvicacm | sixtwoone |
| WHTACMwht | sixon |
| whtacmvtc | sixon |
| whtacmacm | sixone |
| vTChHTwht | twosixsix |
| vTCwHTvTC | twosixtwo |
| vтсwhtacm | twosixone |
| vtcvicwht | twotwo |
| vTCVTCVTC | twot |
| vTCvTCACM | twotwoone |
| vTCACMWHT | twoon |
| vtcacmvic | twoon |
| vTCACMACM | twooneone |
| АСММНTWHT | onesi |
| ACMWHTVTC | onesixtwo |
| АСМННТТСМ | onesixone |
| ACMvTcwht | onetwosix |
| CMvTCVTC |  |
| ACMVTCACM | onetwoone |
| CMACMWHT | one |
|  |  |
|  |  |

