

THE ATBASH CIPHER PROBLEM

Create an implementation of the Atbash cipher, an ancient encryption system created in the Middle East.

The Atbash cipher is a simple substitution cipher that relies on transposing all the letters in the alphabet such that the resulting alphabet is backwards. The first letter is replaced with the last letter, the second with the second-last, and so on.

An Atbash cipher for the Latin alphabet would be as follows:

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: zyxwvutsrqponmlkjihgfedcba

It is a very weak cipher because it only has one possible key, and it is a simple monoalphabetic substitution cipher. However, this may not have been an issue in the cipher's time.

Ciphertext is written out in groups of fixed length, the traditional group size being 5 letters, and punctuation is excluded. This is to make it harder to guess things based on word boundaries.

Input (atbash.txt)

teSt

thequickbrownf,oxjumpsover:thelazydog

Output

gvhg

gsvjf rxpyi ldmul cqfnk hlevi gsvoz abwlt