



Problem 1. «Timing attack»

Anton invented a ciphermachine that can automatically encrypt messages consisting of English letters. Each letter corresponds to the number from 1 to 26 by alphabetical order (1 is for A, 2 is for B, ..., 26 is for Z). The machine encrypts messages letter by letter. It encrypts one letter as follows.

Step 1. If the letter belongs to the special secret set of letters, the machine does not encrypt it, adds the original letter to the ciphertext, and does not go to Step 2; otherwise it goes to Step 2.

Step 2. According to the secret rule, it replaces the current letter with number k by a letter with number ℓ , where ℓ has the same remainder of division by 7, and adds this new letter to the ciphertext.

Anton's classmate Evgeny is interested in different kinds of cryptanalysis that use some physical information about the encryption process. He measured the amount of time that is required for each letter encryption by Anton's ciphermachine and found out that a timing attack can be applied to it!

He captured the ciphertext that Anton sent to his friend and were able to read the message using the information of his measurements!

Could you also decrypt the ciphertext:

Tois keyv is fhve tvvu xust hgvtoed iyife ngfbey!
 Wvat ka rvn knvw owvnt it?

if you know how much time encryption of each message letter took?

