

2246 Cracking the Code

You have been contracted by a terrorist group to crack encrypted transmissions. The only information that the terrorists could give you regarding the encrypted message is that a fixed key-length XOR-encryption algorithm was used to encode it. After a brief search on the 'Net, you find the following definition of XOR-encryption:

Assuming that we have a character $u[i]$ from the unencrypted input stream, and a key k of length l with characters $k[j]$, $0 \leq j < l$, then the encrypted value $e[i]$ is obtained as follows:

$$e[i] = u[i] \text{ XOR } k[i \text{ MOD } l]$$

where MOD is the remainder after integer division (the `%` operator in C, C++ and Java), and XOR is the bitwise XOR operator applied to an 8-bit character (the `^` operator in C, C++ and Java). XOR encryption is a symmetric encryption scheme, so that the message is decoded by encrypting the encrypted message (a second time) with the same key, so that

$$u[i] = e[i] \text{ XOR } k[i \text{ MOD } l]$$

Input and Output

You are given an encrypted input stream of fewer than 30 000 characters. Your program must output the decrypted stream. The stream was encrypted using XOR encryption with a fixed length key of fewer than 30 characters. Each character in the key is unique (appears only once), and is selected from the set 'a'..'z' merged with '0'..'9'.

Your task is to determine the correct key length, and decrypt the encrypted input stream. Your terrorist friends provided you with one last vital piece of information: "The decrypted message will be in English."

It is recommended that you write an XOR encryption program first to aid you in testing your solution.

Sample Input

The output of the XOR encryption algorithm is not normally printable, since it may contain ASCII codes greater than 127. Therefore, the sample-encrypted message below is shown in numerical ASCII values (in decimal) — the actual input file contains the ASCII symbols. If the message "the quick brown fox jumps over the lazy dog" is encrypted using the key '12' (the literal characters '1' and '2', concatenated), the following (binary) file results.

```
69 90 84 18 64 71 88 81 90 18 83 64 94 69 95 18
87 93 73 18 91 71 92 66 66 18 94 68 84 64 17 70
89 87 17 94 80 72 72 18 85 93 86
```

If these values are converted to ASCII symbols and stored in a file (the file length should be exactly 43 bytes), it can be used as input to your program. It is recommended that you first write the encryption algorithm.

Sample Output

Your program should determine the key length to be 2 (you should not output this value), and decrypt the message to yield:

```
the quick brown fox jumps over the lazy dog
```