Baltic OI '01 P2 - Crack the Code

Time limit: 1.0s   **Memory limit:** 256M

Baltic Olympiad in Informatics: 2001 Day 1, Problem 2

Cryptography is the science and technology of coding messages so that only the intended recipient can read them. Cryptanalysis, on the other hand, is the science of breaking the codes. For this problem, assume you're a cryptanalyst hired to break open a series of encrypted messages captured in a police raid to the headquarters of the local mafia. Your colleagues have already reverse engineered the encryption program (see attachments below), and the only thing left to do is to guess the key used to encrypt the files and reverse the algorithm.

Along with the encrypted files, there are also some plaintext files that originate from the same source as the encrypted files and thus have similar structure in terms of language, word usage, etc.

The attached folder below contains the encryption programs implemented in Pascal and C (`crack.pas` and `crack.c`). The pseudocode of these programs is shown below.

$$
\begin{aligned}
&\textbf{File } f_{\text{in}}, f_{\text{out}} \qquad\qquad \triangleright f_{\text{in}} \text{ stores original text}, f_{\text{out}} \text{ stores the encrypted result}\\
&alphabet[0 \ldots 25] \leftarrow \{\texttt{A, B, C, ..., Z}\} \qquad \triangleright \text{ upper-case english alphabet}\\
&len \leftarrow 10, k \leftarrow 0\\
&key[0 \ldots len - 1] \leftarrow \text{ input integer array of size } len\\
&\textbf{while } \text{ not at the end of } f_{in} \textbf{ do}\\
&\quad c \leftarrow \text{ read character from } f_{in}\\
&\quad \textbf{if } alphabet \text{ contains } c \textbf{ then} \qquad\qquad\qquad\qquad \triangleright \text{ shift } c \text{ by } key[k]\\
&\qquad p \leftarrow \text{ position of } c \text{ in } alphabet\\
&\qquad c \leftarrow alphabet[(p + key[k]) \bmod 26]\\
&\qquad k \leftarrow (k + 1) \bmod len\\
&\quad \textbf{end if}\\
&\quad \textbf{print } c \text{ to } f_{\text{out}}\\
&\textbf{end while}
\end{aligned}
$$

Your task is to decrypt the given messages in the attached folder below with the help of the text of same the origin.

Constraints

$1 \le t \le 5$

All letters in the encrypted text files are upper-case.

Input Specification

You are given five data sets.

The input contains one integer t, identifying the number of the current test case.

The data set for test case t consists of the following files:

- t in the encrypted message (f in pseudocode)

- t.in, the encrypted message (f_{out} in pseudocode),
- t.txt, the plaintext file of the same origin as the encrypted message.

For example, if $t = 3$, the encrypted message can be found in `3.in` and the text of the same origin can be found in `3.txt`.

All data set files along with the encryption programs are found in the attachment below.

Output Specification

Decrypt the encrypted message in the file t.in, and output the original message (f_{in} in pseudocode).

Attachment Package

The input files are available here.