

Problem 14: Przesunięcie Cezariańskie

Punkty: 40

Autor: Carlos J. Sepulveda, Orlando, Floryda, Stany Zjednoczone

Wprowadzenie

Szyfr Cezara to prosty szyfr podstawieniowy, który zastępuje każdą literę alfabetu inną literą, odpowiednio do zadanego przesunięcia. Najczęstsze stosowane przesunięcie to 3, gdzie A jest zastępowane D, B jest zastępowane E itd. aż do zawinięcia alfabetu tak, że XYZ jest zastępowane ABC.

ABCDEF GHIJ KLMNOP QRSTUV WXYZ
DEFGHI JKL MNOPQR STUVWX YZABC

Niestety ten szyfr jest tak dobrze znany i prosty do złamania, że jego użyteczność jest niewielka... spróbujmy utrudnić sprawę.

Opis problemu

Opisany powyżej szyfr Cezara to szyfr monoalfabetyczny - każdą literę zastępuje inna. W naszym wariantcie każda litera będzie szyfrowana w inny sposób, w zależności od zadanego zestawu wartości i kierunków. Litery mogą być przesuwane w lewo (do tyłu) lub w prawo (do przodu) o wielkość z przedziału 1-25.

Przykładowo, literę A można by zaszyfrować na kilka sposobów.

- Przesunięcie o 3 w prawo daje D, jak w tradycyjnym przesunięciu Cezariańskim.
- Przesunięcie o 3 w lewo daje X, po zawinięciu alfabetu.
- Przesunięcie o 10 w prawo daje K, jedenastą literę alfabetu.
- Przesunięcie o 10 w lewo daje Q, dziesięć liter przed A (po zawinięciu).

Przesunięcia i ich kierunek będą podawane w postaci liczb: przesunięcie w zakresie od 1 do 25 włącznie, a kierunek w postaci 0 (w lewo) lub 1 (w prawo). Te zestawy danych mogą mieć różną długość, ale zwykle będą krótsze od wiadomości, którą próbujemy odszyfrować. Po dotarciu do końca zestawu należy go zapętlić tak, by przejść ponownie do początku.

Mając zadaną zaszyfrowaną wiadomość oraz przesunięcie i jego kierunek wasz zespół ma za zadanie odszyfrować wiadomość. Spacje i inne znaki przestankowe w wiadomości pozostawiacie bez zmian; nie zmieniacie również pozycji w zestawach kluczy.

Przykładowe dane wejściowe

Pierwszy wiersz danych wejściowych programu, otrzymanych przez standardowy kanał wejściowy, będzie zawierał dodatnią liczbę całkowitą oznaczającą liczbę przypadków testowych. Każdy przypadek testowy będzie zawierał trzy wiersze:

- Zaszyfrowaną wiadomość o dowolnej długości zawierającą wielkie litery, spacje i znaki przestankowe.
- Listę co najmniej dwóch dodatnich liczb całkowitych od 1 do 25 włącznie, oddzielonych spacjami, odpowiadających wartościom przesunięcia, które zastosowano do zaszyfrowania wiadomości.
- Listę co najmniej dwóch liczb całkowitych, równych 0 lub 1, oddzielonych spacjami, odpowiadających kierunkom przesunięcia, które zastosowano do zaszyfrowania wiadomości.

```
3
EDEPCG
1 1 2
1 0 1
EDENEC
1 1 2
1 0
DYA! EZP?
1 2
1 0 0
```

Przykładowe dane wyjściowe

W każdym przypadku testowym program musi wyświetlić niezaszyfrowaną wiadomość. Wiadomość powinna być wyświetlana w jednym wierszu, małymi literami, z zachowaniem spacji i znaków przestankowych.

```
decode
decode
cab! car?
```