Szyfr Gronsfelda

Twierdzi się, że kiedy Cezar prowadził wojnę w Galii, w obawie przez ujawnieniem nieprzyjacielowi swoich zamiarów całą korespondencję z dowódcami polowymi prowadził stosując szyfr, nazwany potem jego imieniem. Pomysł był prosty – każdą literę w wiadomości Cezar zastępował taką, która w alfabecie występowała jako następna. W ten sposób **A** zamieniało się na **B**, **B** na **C**, itd. Wyjątek czyniono dla **Z**, którą Cezar zastępował literą **A**. Jeśli weźmiemy pod uwagę, że ówcześni Rzymianie nie używali żadnych znaków przestankowych, nie znali małych liter (używali tylko takich, które my znamy pod nazwą liter wielkich), ba (niewiarygodne, ale prawdziwe) nie stosowali spacji, a do zapisu liczb z oczywistych powodów używali nie cyfr, a liter, to widzimy, że taki sposób był sprawny i wydajny. Na przykład:

tekst jawny	**CEZAR**
tekst zaszyfrowany	**DFABS**

Dzisiaj o takim szyfrze mówi się, że jest szyfrem Cezara o przesunięciu jeden – to '*jeden*' mówi, że zamiast litery oryginalnej bierzemy literę odległą od niej w alfabecie o jeden. Możemy oczywiście wyobrazić sobie szyfr Cezara o innym przesunięciu, np. równym trzy:

tekst jawny	**CEZAR**
tekst zaszyfrowany	**FHCDU**

Jakie by jednak nie było wybrane przesunięcie, szyfr Cezara ciągle ma jedną poważną wadę – zachowuje częstość występowania znaków. Dzieje się tak dlatego, że pewnej literze w tekście jawnym zawsze odpowiada taka sama litera w tekście zaszyfrowanym. Jeśli wiemy, jakie litery w pewnym języku występują najczęściej (albo najrzadziej), to możemy podjąć próbę złamania takiego szyfru i jak pokazuje praktyka, jeśli tylko szyfrogram będzie odpowiednio długi, mamy duże szanse powodzenia.

Ponad półtora tysiąca lat po Cezarze, Holender Josse Maximilian van Gronsfeld (1598-1667), uczestnik wojny trzydziestoletniej, wynalazł (dodajmy, że nie był pierwszy – przed nim na nieco inny sposób dokonali tego Blaise Vigener i Giovan Batista Belaso) sposób ominięcia tej właśnie słabości szyfru Cezara. Zaproponował on, aby dla szyfrowania kolejnych liter używać innego przesunięcia – takiego, jakie wynika z klucza, który jest znany tylko nadawcy i odbiorcy. Sam klucz jest liczbą, której kolejne cyfry interpretuje się jako wartość przesunięcia stosowaną dla kolejnych znaków. Dodatkowo wprowadza się zasadę mówiącą, że jeśli klucz jest krótszy niż tekst (zapewne dotyczy to zdecydowanej większości szyfrowanych wiadomości), to w chwili, kiedy wykorzystamy wszystkie cyfry klucza, wracamy do jego początku. Popatrzmy na przykład:

tekst jawny	**CEZAR**

klucz	123
tekst zaszyfrowany	**DGCBT**

Znając już sposób szyfrowania metodą Gronsfelda, bez problemu ustalisz, jak wygląda procedura deszyfracji.

Polecenie: napisz program, który szyfruje i deszyfruje wiadomości,wykorzystując metodę Gronsfelda.

Dane wejściowe: 3 wiersze tekstu, zawierające kolejno:

1. słowo SZYFRUJ lub DESZYFRUJ, oznaczające odpowiednio polecenie zaszyfrowania lub odszyfrowania wiadomości;
2. liczbę całkowitą *k*, będącą kluczem szyfru Gronsfelda (*0 <= k <= 1000000000*);
3. tekst do szyfrowania/deszyfrowania o nieznanej z góry długości, składający się tylko i wyłącznie z wielkich liter alfabetu łacińskiego.

Dane wyjściowe: jeden wiersz tekstu, wynikający z szyfrowania/deszyfrowania tekstu podanego programowi w trzecim wierszu standardowego wejścia.

Przykład:

Wejście:

SZYFRUJ

12340

ALAMAKOTA

Wyjście:

BNDQALQWE

Wejście:

DESZYFRUJ

12340

BNDQALQWE

Wyjście:

ALAMAKOTA