

# Zadanie: VIGENER

## Szyfr Vigenera

CPSPC 2010

CPSPC 2010, dzień 1.

21.06.2010

Dostępna pamięć: 64 MB. Maksymalny czas działania: 5 s.

Prawdopodobnie wszyscy słyszeli o szyfrze Vigenera. Szyfrowanie polega na dodawaniu do siebie kolejnych liter tekstu oraz cyklicznie powtarzającego się klucza. Litery dodajemy do siebie analogicznie do dodawania liczb z zakresu 0 do 25 w arytmetyce modulo 26. Na przykład dla tekstu CPSPCISANABBREVIATION i klucza CPSPC otrzymujemy zakodowaną wiadomość EEKEEKHSCCDQJTXKPLXQP (patrz rysunek).

C	P	S	P	C	C	P	S	P	C	C	P	S	P	C	C	P	S	P	C	
C	P	S	P	C	I	S	A	N	A	B	B	R	E	V	I	A	T	I	O	N
E	E	K	E	E	K	H	S	C	C	D	Q	J	T	X	K	P	L	X	Q	P

Twoim zadaniem jest odkodować zaszyfrowany tekst, mając daną długość klucza oraz częstotliwość występowania wszystkich par liter w języku, z którego pochodzi tekst. W praktyce takie podejście daje zaskakująco dobre wyniki.

Otrzymasz tekst zakodowany szyfrem Vigenera przy użyciu klucza długości  $K$ . Wiadomo, że pierwotny tekst nie zawierał spacji. Ponadto podana będzie częstotliwość występowania wszystkich par liter w języku oryginalnego tekstu. Znajdź taki klucz, dla którego odszyfrowany tekst maksymalizuje sumę częstotliwości występowania par liter.

## Wejście

W pierwszym wierszu wejścia znajdują się dwie liczby całkowite  $K$  ( $K \leq 5000$ ) i  $N$  oznaczające odpowiednio długość klucza oraz liczbę par liter, dla których znany jest częstotliwość występowania. W każdym z kolejnych  $N$  wierszy znajduje się para wielkich liter oraz liczba określająca częstotliwość ich występowania. Częstotliwość wyrażona jest dodatnią liczbą całkowitą nie większą niż  $10^8$ ; czym większa częstotliwość, tym większe prawdopodobieństwo wystąpienia tej pary. W ostatnim wierszu wejścia znajduje się zaszyfrowany tekst. Składa się on z co najwyżej 10000 wielkich liter alfabetu angielskiego.

## Wyjście

W pierwszym i jedynym wierszu wyjścia należy wypisać najbardziej prawdopodobny klucz, którym zaszyfrowano tekst, czyli taki, że po rozszyfrowaniu powstanie tekst o maksymalnej sumie częstotliwości. Jeśli jest wiele rozwiązań o maksymalnym prawdopodobieństwie, można wypisać dowolne z nich.

Możesz założyć, że dla optymalnego wyniku, suma częstotliwości par liczb w słowie nie przekroczy  $10^8$ .

Dla danych wejściowych:

5 6

TE 2

YP 1

XT 1

RY 1

PT 1

OI 1

JTDAQKPETPEGQEVGSLTZV

poprawnym wynikiem jest:

CPSPC

**Wyjaśnienie do przykładu:** Wejście w przykładzie odpowiada tekstowi HELLOIAMENCRYPTEDTEXT zakodowanemu kluczem CPSPC. Suma częstotliwości występowania liter dla tego klucza to 9.