Ewentualne potrzebne pliki: www.code.kopernik-leszno.pl/zbiorzadan/pliki.zip

Zadanie 77.

Wiązka zadań *Szyfr Vigenère'a*

W zadaniu rozważamy teksty zbudowane tylko z wielkich liter alfabetu angielskiego, znaków odstępu i znaków przestankowych (przecinek, kropka). Oto litery alfabetu i numery ich pozycji w alfabecie:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Szyfrowanie Vigenère'a polega na zastąpieniu każdej litery tekstu źródłowego literą odległą od niej cyklicznie w alfabecie o k pozycji.

Wartość k nie jest z góry ustalona dla całego tekstu źródłowego, lecz dla każdej litery w tekście jest określana osobno, w oparciu o słowo przyjęte jako klucz szyfrowania.

Przystępując do szyfrowania, należy przyporządkować kolejnym literom tekstu źródłowego kolejne litery klucza, chodząc po nim cyklicznie, jeśli jest krótszy od szyfrowanego tekstu. Znaki inne niż litery nie są szyfrowane, pomijamy je podczas przypisywania liter klucza. **Pozycja litery klucza** w alfabecie jest tą wartością ***k***, o jaką należy wykonać przesunięcie względem litery tekstu źródłowego w celu znalezienia odpowiadającej jej litery szyfru.

Przykład

tekst źródłowy: `"JEST OK"`, klucz: `"EWA"`

tekst źródłowy	J	E	S	T	spacja	O	K
Klucz	E	W	A	E		W	A
pozycja litery klucza	4	22	0	4		22	0
Szyfr	J→4 = **N**	E→22=**A**	S→0 = **S**	T→4 = **X**	spacja	O→22=**K**	K→0 = **K**

wynik szyfrowania: `"NASX KK"`.

Napisz w wybranym języku programowania program, który wyznaczy rozwiązania zadań podanych niżej. Wszystkie wyniki zapisz w pliku tekstowym `Vigenere_wyniki.txt`, wyraźnie oddzielając odpowiedzi do poszczególnych zadań. Do oceny oddaj ten plik oraz plik (pliki) zawierający reprezentację komputerową rozwiązania.

77.1.

W pliku `dokad.txt` znajduje się jeden wiersz z tekstem. Długość tekstu nie przekracza 1024 znaków. Należy zaszyfrować ten tekst metodą Vigenère'a, używając jako klucza słowa: "LUBIMYCZYTAC".

a) Podaj liczbę powtórzeń klucza niezbędną do zaszyfrowania całego tekstu źródłowego (uwzględniając w nich ostatnie rozpoczęte powtórzenie).

b) Podaj zaszyfrowany tekst i zapisz go w pliku z odpowiedziami.

77.2.

W pliku `szyfr.txt` zapisano dwa wiersze. W pierwszym wierszu znajduje się tekst zaszyfrowany metodą Vigenère'a. W drugim wierszu znajduje się klucz użyty do tego szyfrowania.

Szyfr zawiera wiele słów. Jego łączna długość nie przekracza 1024 znaków. Szyfrowaniu podlegały tylko wielkie litery tekstu, zaś odstępy i znaki przestankowe pozostały bez zmiany.

Odszyfruj tekst i umieść jego postać źródłową w pliku z odpowiedziami.

77.3.

a) Podaj liczby wystąpień poszczególnych liter A, B, ..., Z w treści szyfru zawartego w pierwszym wierszu pliku `szyfr.txt`.

b) Chcąc złamać szyfr Vigenère, nie znając klucza, w pierwszym kroku należy oszacować długość klucza (rozumianą jako liczba znaków). Istnieje przybliżony wzór na szacunkową długość klucza *d* danego szyfru Vigenère'a dla tekstu nad alfabetem 26-literowym. Oszacowanie jest tym lepsze, im dłuższy jest szyfr.

$$d = \frac{0{,}0285}{\kappa_o - 0{,}0385}$$

gdzie κ_o to indeks koincydencji znaków obliczany następująco:

$$\kappa_o = \frac{l_A * (l_A - 1) + l_B * (l_B - 1) + \cdots + l_Z * (l_Z - 1)}{n * (n - 1)}$$

n — łączna liczba wystąpień **wszystkich liter** w tekście szyfru (nie liczymy odstępów i znaków przestankowych),

$l_A, l_B, \ldots, l_Z$ — liczby wystąpień **poszczególnych liter** `A`, `B`, …, `Z` w tekście szyfru.

Wykorzystując powyższe wzory, wyznacz szacunkową długość klucza dla szyfru danego w pierwszym wierszu pliku `szyfr.txt` i porównaj z dokładną długością klucza umieszczonego w drugim wierszu tego pliku. Wypisz obie wartości, wartość szacunkową zaokrąglij do 2 cyfr po przecinku.

Publikacja opracowana przez zespół koordynowany przez **Renatę Świrko** działający w ramach projektu *Budowa banków zadań* realizowanego przez Centralną Komisję Egzaminacyjną pod kierunkiem Janiny Grzegorek.

Autorzy
dr Lech Duraj
dr Ewa Kołczyk
Agata Kordas-Łata
dr Beata Laszkiewicz
Michał Malarski
dr Rafał Nowak
Rita Pluta
Dorota Roman-Jurdzińska

Komentatorzy
prof. dr hab. Krzysztof Diks
prof. dr hab. Krzysztof Loryś
Romualda Laskowska
Joanna Śmigielska

Opracowanie redakcyjne
Jakub Pochrybniak

Redaktor naczelny
Julia Konkołowicz-Pniewska

Zbiory zadań opracowano w ramach projektu *Budowa banków zadań*,
Działanie 3.2 Rozwój systemu egzaminów zewnętrznych,
Priorytet III Wysoka jakość systemu oświaty,
Program Operacyjny Kapitał Ludzki

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

CENTRALNA
KOMISJA
EGZAMINACYJNA

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY