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

Zadanie 75.

Wiązka zadań *Szyfr afiniczny*

Dany jest tekst złożony ze słów zbudowanych z małych liter alfabetu angielskiego. Metoda szyfrowania afinicznego — dla której *kluczem szyfrującym* są dwie liczby całkowite A i B — polega na wykonaniu kolejno następujących operacji:

- zastąpienia kolejnych liter alfabetu liczbami od 0 do 25: 'a' przez 0, 'b' przez 1, 'c' przez 2 itd. według przyporządkowania przedstawionego w poniższej tabeli:

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

- pomnożenia liczby odpowiadającej każdej literze przez A i dodania otrzymanego wyniku do B,

- zamiany otrzymanych liczb z powrotem na litery; jeśli liczba jest większa niż 25, bierze się jej resztę z dzielenia przez 26.

Parametry klucza, czyli liczby A i B, powinny być liczbami całkowitymi z przedziału [0, 25].

Dla przykładu, jeśli kluczem szyfrującym jest (3, 7), czyli A = 3, zaś B = 7, to litera 'n' jest najpierw zastępowana liczbą 13. Po pomnożeniu jej przez A i dodaniu B otrzymujemy wynik równy 46. W następnym kroku otrzymujemy literę o numerze 46 – 26 = 20, czyli 'u'.

Okazuje się, że do odszyfrowania szyfru afinicznego można zastosować tę samą metodę, być może z innym kluczem. Na przykład, jeśli napis zaszyfrujemy kluczem (3, 7), to aby go odszyfrować, stosujemy ten sam algorytm z kluczem (9, 15). Dla przykładu, deszyfrując literę 'u' z kluczem (9, 15), otrzymamy liczbę 20 * 9 + 15 = 195, czyli literę 'n', jako że 195 mod 26 = 13. Klucz (9,15) jest wówczas *kluczem deszyfrującym* dla klucza (3,7).

Napisz program(y), który poda odpowiedzi do poniższych zadań. Odpowiedzi zapisz do pliku `wyniki.txt`.

75.1.

W pliku `tekst.txt` dany jest, w pojedynczym wierszu, tekst złożony z dokładnie 805 słów zapisanych małymi literami alfabetu angielskiego, oddzielonych znakami odstępu. Żadne słowo nie jest dłuższe niż 15 znaków.

Znajdź i wypisz te słowa, których zarówno pierwszą, jak i ostatnia literą jest 'd'.

75.2.

Zaszyfruj szyfrem afinicznym o kluczu (5, 2) te słowa z pliku `tekst.txt`, które składają się z co najmniej 10 liter. Wypisz je w postaci zaszyfrowanej, po jednym w wierszu.

75.3.

Plik `probka.txt` składa się z 5 wierszy, każdego zawierającego dwa napisy. Pierwszy z nich to pewne słowo zapisane tekstem jawnym, drugi zaś to to samo słowo zaszyfrowane za pomocą szyfru afinicznego (każde słowo innym kluczem).

Dla każdego z tych słów znajdź i wypisz klucz szyfrujący oraz klucz deszyfrujący.

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