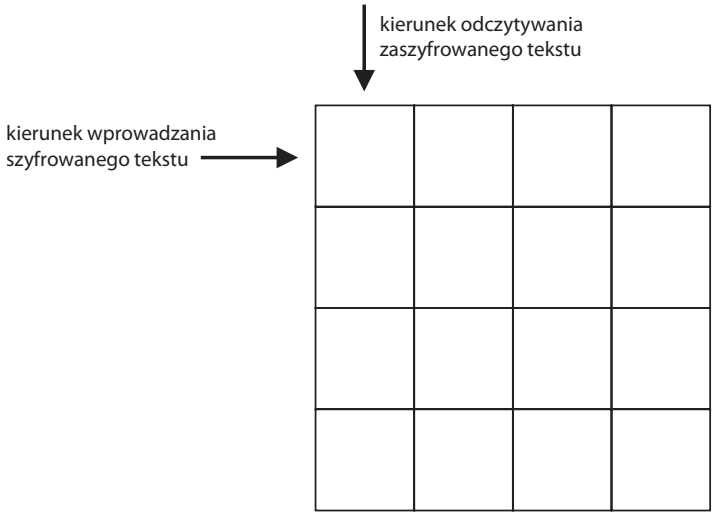
Egzamin maj 2010 r. Arkusz I, poziom rozszerzony, zadanie 1. SZYFR PRZESTAWIENIOWY

Szyfrowanie przestawieniowe jest klasyczną metodą szyfrowania polegającą na zmianie kolejności liter w szyfrowanym tekście. Często używa się reguł zamiany opartych na różnych figurach geometrycznych — w tym zadaniu użyjemy kwadratu. Szyfrowanie będzie polegało na wprowadzeniu tekstu do kwadratowej tablicy szyfrującej o wymiarach $n \times n$ po kolei wierszami, a następnie odczytaniu tekstu z tablicy kolumnami od lewej do prawej. Wymiar n tablicy jest najmniejszą liczbą, przy której tekst zmieści się w całości w kwadracie $n \times n$. W przypadku gdy tekst jest krótszy i nie wypełnia wszystkich pól tablicy, puste pola uzupełnia się znakami odstępu. W tym zadaniu znaki odstępu będziemy oznaczać _.



Przykład

Załóżmy, że tekst **ALGORYTM_PRZESTAWIENIOWY** ma być zaszyfrowany w tablicy kwadratowej. Liczba znaków w tekście do zaszyfrowania jest równa 24, czyli tablica szyfrująca ma wymiary 5×5 . Ostatni element tablicy będzie uzupełniony znakiem odstępu. Tekst zapisujemy do tablicy wierszami.

A	L	G	O	R
Y	T	M	_	P
R	Z	E	S	T
A	W	I	E	N
I	O	W	Y	_

Następnie odczytujemy zaszyfrowany tekst kolumnami:

AYRAILTZWOGMEIWO_SEYRPTN_

a) Podaj wzór na liczbę wierszy i kolumn tablicy kwadratowej używanej do szyfrowania tekstu o długości d znaków lub opisz algorytm wyznaczania tej liczby (w postaci listy kroków, schematu blokowego lub w wybranym języku programowania).

b) Do zaszyfrowania pewnego cytatu z Sokratesa użyto metody opisanej w podpunkcie a). Rozszyfruj ten cytat. Poniższy szyfr składa się z 64 znaków.

BTLLTU_ĘŁ_EOYPM_ĄPJZLCYNDREOKYLI_ZMFO_ĄGJY_Ó_N_DEWFWGISYSII_ŁEI_

c) Zapisz algorytm (w postaci listy kroków, schematu blokowego lub w wybranym języku programowania), który szyfruje zadany tekst sposobem opisanym w tym zadaniu i jest zgodny z poniższą specyfikacją.

Specyfikacja

Dane:

d — dodatnia liczba całkowita, długość tekstu do zaszyfrowania

tekst[1…*d*] — tablica zawierająca tekst do zaszyfrowania, gdzie *tekst*[*i*], to *i*-ty znak w tekście do zaszyfrowania

Wynik:

s — dodatnia liczba całkowita, długość tekstu po zaszyfrowaniu

szyfr[1…*s*] — tablica zawierająca tekst po zaszyfrowaniu, gdzie *szyfr*[*i*], to *i*-ty znak w tekście po zaszyfrowaniu