

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

Zadanie 76.

Wiązka zadań Szyfr

Rozważamy szyfrowanie przestawieniowe, w którym kluczem jest n -elementowa tablica zawierająca różne liczby całkowite z przedziału $[1, n]$. Na przykład kluczem 5-elementowym może być tablica $[3, 2, 5, 4, 1]$.

Szyfrowanie napisu A (o długości co najmniej n) kluczem n -elementowym $P[1..n]$ odbywa się w następujący sposób:

- pierwsza litera słowa A zamieniana jest miejscami z literą na pozycji $P[1]$,
- następnie druga litera słowa A zamieniana jest z literą na pozycji $P[2]$
- itd.

Uzyskane na końcu słowo jest szyfrem napisu A z kluczem P .

Jeśli napis A ma więcej niż n liter, to po n -tym kroku powyższego algorytmu kolejną literę zamieniamy znów z literą na pozycji $P[1]$ itd. Oznacza to, że w i -tym kroku zamieniamy litery na pozycjach i oraz $P[1+(i-1) \bmod n]$.

Przykład

Poniższa tabelka ilustruje szyfrowanie słowa „INFORMATYKA” kluczem P równym $[3, 2, 5, 4, 1]$:

i	1	2	3	4	5	6	7	8	9	10	11
$P[1+(i-1) \bmod n]$	3	2	5	4	1	3	2	5	4	1	3
Słowo	I	N	F	O	R	M	A	T	Y	K	A
Krok 1	F	N	I	O	R	M	A	T	Y	K	A
Krok 2	F	N	I	O	R	M	A	T	Y	K	A
Krok 3	F	N	R	O	I	M	A	T	Y	K	A
Krok 4	F	N	R	O	I	M	A	T	Y	K	A
Krok 5	I	N	R	O	F	M	A	T	Y	K	A
Krok 6	I	N	M	O	F	R	A	T	Y	K	A
Krok 7	I	A	M	O	F	R	N	T	Y	K	A
Krok 8	I	A	M	O	T	R	N	F	Y	K	A
Krok 9	I	A	M	Y	T	R	N	F	O	K	A
Krok 10	K	A	M	Y	T	R	N	F	O	I	A
Krok 11	K	A	A	Y	T	R	N	F	O	I	M

Napis „KAAYTRNFOIM” jest zatem szyfrem napisu „informatyka” z kluczem $[3, 2, 5, 4, 1]$.
Napisz program(-y), który da odpowiedzi do poniższych zadań.

76.1.

W pliku `szyfr1.txt` dane są:

- w wierszach o numerach od 1 do 6 — napisy złożone z 50 liter alfabetu łacińskiego;
- w wierszu nr 7 — klucz 50-elementowy; liczby oddzielone są pojedynczym odstępem.

Zaszyfruj wszystkie sześć napisów zgodnie z opisaną metodą. Wynik, czyli zaszyfrowane napisy, zapisz w osobnych wierszach w pliku `wyniki_szyfr1.txt`.

76.2.

W pliku `szyfr2.txt` dane są:

- w pierwszym wierszu — napis złożony z 50 liter alfabetu łacińskiego;
- w drugim wierszu — klucz 15-elementowy; liczby oddzielone są pojedynczym odstępem.

Zaszyfruj dany napis zgodnie z opisaną metodą. Wynik, czyli zaszyfrowany napis, zapisz w pliku `wyniki_szyfr2.txt`.

76.3.

W pliku `szyfr3.txt` dany jest napis złożony z 50 liter alfabetu łacińskiego. Napis ten powstał po zaszyfrowaniu pewnego napisu A kluczem $[6, 2, 4, 1, 5, 3]$.

Podaj napis *A*. Wynik zapisz w pliku `wyniki_szyfr3.txt`.

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