

Zadanie 30.**Wiązka zadań Szyfrowanie**

Szyfrowanie z kluczem k (k — liczba całkowita większa lub równa 0) polega na zastąpieniu każdego znaku wiadomości jawnej innym znakiem o pozycji przesuniętej w alfabecie o k znaków względem znaku szyfrowanego. Przy szyfrowaniu znaku należy postępować w sposób cykliczny, tzn. po osiągnięciu końcowego znaku alfabetu należy powrócić na jego początek. Rozważamy tylko wielkie litery alfabetu angielskiego, tj. litery o kodach dziesiętnych ASCII od 65 (dla znaku A) do 90 (dla znaku Z).

30.1.

Mając do dyspozycji funkcję $kod(x)$, która dla danego znaku x podaje dziesiętny kod ASCII tego znaku (np. $kod(A) = 65$), oraz funkcję $znak(y)$, która dla danego dziesiętnego kodu ASCII podaje znak odpowiadający temu kodowi (np. $znak(77) = M$), napisz funkcję $szyfruj(zn, k)$, szyfrującą znak zn szyfrem z kluczem k .

Przykład działania funkcji: $szyfruj(M, 327) = B$.

30.2.

Aby utrudnić proces deszyfrowania, postanowiono dla każdego znaku w słowie zastosować inny klucz. Kluczem znaku w słowie będzie numer jego pozycji w tym słowie.

Przykład: w słowie BIT, dla znaku B mamy $k=1$, dla I — $k=2$, a dla T — $k=3$. Zasyfrowane słowo BIT to CKW.

Uzupełnij poniższą tabelę. Zasyfruj opisanym sposobem podane słowo jawne oraz odszyfruj słowo zasyfrowane.

Słowo jawne	Słowo zasyfrowane
INFORMATYKA	
	LQPTZZLZ

30.3.

Dane jest słowo S zaszyfrowane sposobem opisanym w zadaniu 2. Podaj algorytm (w postaci pseudokodu lub kodu wybranego języka programowania) deszyfrujący słowo S .

Dane:

- n — liczba znaków w słowie S ($n > 0$)
- $S[1..n]$ — zaszyfrowane słowo

Wynik:

- $J[1..n]$ — słowo jawne, które po zaszyfrowaniu daje słowo S

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