ZADANIE 10
Szyfr Playfair
dla I klasy gimnazjum
z podstaw algorytmiki (pakiet B2)

1. Metryczka zadania:

Oznaczenie zadania (numer)	Zakres materiału (wg podstawy programowej)	Szacowana łatwość (w skali: b. łatwe, łatwe, średnio-trudne, trudne, b. trudne)	Maksymalna liczba punktów	Szacowany czas potrzebny na rozwiązanie (w min)
10	Rozwiązywanie problemów i podejmowanie decyzji z wykorzystaniem komputera, stosowanie podejścia algorytmicznego. Uczeń: formułuje ścisły opis prostej sytuacji problemowej, analizuje ją i przedstawia rozwiązanie w postaci algorytmicznej.	trudne	8	15

Uczeń:

- formułuje ścisły opis prostej sytuacji problemowej, analizuje ją i przedstawia rozwiązanie w postaci algorytmicznej;
- opisuje sposób znajdowania wybranego elementu w zbiorze nieuporządkowanym i uporządkowanym, opisuje algorytm porządkowania zbioru elementów;
- bierze udział w dyskusjach na forum.

2. Treść zadania:

Jedną z metod szyfrowania informacji jest Szyfr Playfair Polega on na zastąpieniu par liter tekstu jawnego inną parą liter. Użyjmy jako słowa-klucza słowa ***MYSZ***. Zatem pierwszą czynnością będzie zapisanie liter alfabetu w kwadracie 5 x 5, zaczynając od słowa. Po wpisaniu do tablicy słowa kluczowego wpisujemy kolejne litery alfabetu zaczynając od A, pomijając litery, które wystąpiły już w słowie kluczowym, litery I i J wpisujemy do jednej komórki.

M	Y	S	Z	A
B	C	D	E	F
G	H	I/J	K	L
N	O	P	Q	R
T	U	V	W	X

Projekt „Żyj twórczo. Zostań M@T.e-MANIAKIEM" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Potem dzielimy tekst, który mamy zamiar zaszyfrować na pary liter. Każda z par powinna się składać z dwóch różnych od siebie liter. W razie potrzeby w celu rozdzielenia pary takich samych liter wstawiamy pomiędzy nie znak **x**. Literę **x** dodajemy także na końcu wtedy, gdy ostatnia litera w tekście nie ma pary. Następnie przystępujemy do właściwego szyfrowania. Pary liter możemy podzielić na trzy grupy:

- obie litery są w tym samym wierszu,
- obie litery są w tej samej kolumnie,
- pozostałe.

Jeśli obie litery są w tym samym wierszu, zastępujemy je sąsiadującymi z nimi literami z prawej strony; na przykład NO zamienia się w OP. Jeżeli jedna z liter znajduje się na samym końcu wiersza, zastępujemy ją pierwszą literą w tym wierszu. Jeśli obie litery znajdują się w tej samej kolumnie, powinny zostać zastąpione przez litery leżące pod nimi; np. GN zmienia się w NT. Jeżeli któraś litera znajduje się na końcu kolumny, zastępujemy ją pierwszą literą w kolumnie.

Zupełnie inna jest sytuacja, kiedy każda z liter znajduje się w innym wierszu i innej kolumnie. W takim wypadku, aby zaszyfrować pierwszą literę, idziemy wzdłuż wiersza, aż dotrzemy do kolumny, która zawiera drugą literę. Litera na skrzyżowaniu wiersza z kolumną zastępuje pierwszą literę. W celu zaszyfrowania drugiej z liter, szukamy wzdłuż wiersza kolumny, w której znajduje się pierwsza litera. Znak ze skrzyżowania reprezentuje drugą literę np. PL zastępujemy parą liter RI.

Przykład:
Tekst jawny: wakacje.
Tekst ten dzielimy na grupy dwuznakowe, na końcu dopisujemy x. Otrzymujemy: wa–ka–cj-ex
Tekst zaszyfrowany: xz-lz-dh-fw

a) W oparciu o utworzony alfabet szyfrowy zaszyfruj słowo INFORMATYKA.
b) Korzystając z utworzonego alfabety odszyfruj słowo YMMBFA.
c) Utwórz nowy alfabet szyfrowy na podstawie słowa kluczowego ZEGAR i zaszyfruj metodą Playfair słowo PAJACYK.

3. Modelowe rozwiązanie (jeżeli istnieją różne sposoby rozwiązania to przynajmniej komentarz w tej kwestii):
   a) GPCRNAMXZHFA
   b) MATMA

Z	E	G	A	R
B	C	D	F	H

Projekt „Żyj twórczo. Zostań M@T.e-MANIAKIEM" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚĆ
WYŻSZA SZKOŁA EUROPEJSKA IM. KS. JÓZEFA TISCHNERA
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY

I/J	K	L	M	N
O	P	Q	S	T
U	V	W	X	Y

Tekst jawny: PA-JA-CY-KX
Tekst po zaszyfrowaniu: SE-MZ-HV-MV

4. Schemat oceniania:

Nr podpunktu	a)	b)	c)
Max liczba pkt	2	2	4

5. Propozycje wykorzystania:

Zadanie przeznaczone jest do samodzielnej pracy jako zadanie dodatkowe lub praca domowa. Wymaga od ucznia skupienia i przeanalizowania algorytmu szyfrowania. Oczywiście zadanie może być opublikowane na Moodlu gdzie uczeń w razie potrzeby może komunikować się z nauczycielem poprzez zapytanie na forum lub system indywidualnych wiadomości.

Projekt „Żyj twórczo. Zostań M@T.e-MANIAKIEM" jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚĆ
WYŻSZA SZKOŁA EUROPEJSKA IM. KS. JÓZEFA TISCHNERA
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY