**ZADANIE 5**
**Twierdza szyfrów**
**- dedykowane kołom informatycznym lub klasom mat.-inf. -**
**z algorytmiki języka programowania C++ (pakiet B6)**

## 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) |
|---|---|---|---|---|
| 5 | Rozwiązywanie problemów i podejmowanie decyzji z wykorzystaniem komputera, stosowanie podejścia algorytmicznego. **Uczeń** stosuje podejście algorytmiczne do rozwiązywania problemu i zapisuje go w wybranej notacji; opisuje podstawowe algorytmy i stosuje: algorytmy kompresji i szyfrowania, np.: szyfr przestawieniowy. **Uczeń** dobiera odpowiednie struktury danych do realizacji algorytmu. | trudne | 8 | 12 |

**Uczeń:**

- wykorzystuje technologie komunikacyjno-informacyjne do komunikacji i współpracy z nauczycielami i innymi uczniami, a także z innymi osobami, jak również w swoich działaniach kreatywnych;
- formułuje specyfikacje dla wybranych sytuacji problemowych;
- projektuje rozwiązanie: wybiera metodę rozwiązania, odpowiednio dobiera narzędzia komputerowe, tworzy projekt rozwiązania;
- realizuje rozwiązanie na komputerze - za pomocą oprogramowania aplikacyjnego lub języka programowania.

## 2. Treść zadania:

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

Wśród metod szyfrowania wyróżniamy **metody podstawieniowe** (np. **Szyfr Cezara**) lub **przestawieniowe** (metoda polegająca na zmianie kolejności liter w szyfrowanym tekście). Zadanie nasze będzie polegało na zaszyfrowaniu tekstu metodą przestawieniową tzw. **metodą płotu**, gdzie naszym kluczem szyfrowania będzie liczba płotków. Metodę tą najłatwiej wyjaśnić na przykładzie. Zaszyfrujmy tekst: ***najbardziej lubię lody czekoladowe***. Niech liczba płotów wynosi ***3***. Proces szyfrowania polega na zapisywaniu pierwszej litery tekstu w pierwszym płotku, drugiej w drugim, trzeciej w trzecim, a gdy braknie płotków zaczynamy uzupełniać płotki ponownie od pierwszego do ostatniego i tak do wyczerpania znaków w tekście. Spacje pomijamy. Otrzymujemy płotki:

I nbdeuedzode
II aazjblyelo
IIIjriliockaw

Następnie przepisujemy zawartość pierwszego płotka, za nim drugiego, a następnie trzeciego. Dla naszego tekstu otrzymamy następujący szyfrogram:

***nbdeuedzodeaazjblyelojriliockaw***

a) Napisz program, który będzie szyfrował teksty wyżej opisaną metodą. Długość tekstu nie może przekroczyć 100 znaków, a liczbę płotów będzie nie większa niż 10.
b) Zaproponuj metodę rozszyfrowywania tak zapisanej wiadomości. Opisz tą metodę.

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

- **Zadanie5_.cpp**.
- Zadanie to można rozwiązać na wiele sposobów, np. wyliczając liczbę elementów w każdym płotku i przeskakując po tekście co pewną liczbę znaków.
- Do rozwiązania zadania można wykorzystać typ danych string i związaną z nim bibliotekę.

4. Schemat oceniania:

a) 10 pkt za poprawny kryptograf. Należy przetestować program dla różnej liczby płotków i dla sytuacji, w której nie wszystkie płotki są tej samej długości. Poszczególne elementy zadania należy punktować w zależności od wybranej metody - należy zwrócić uwagę na wartości brzegowe.
b) Opis metody:
   a. Obliczamy liczbę znaków w zaszyfrowanym tekście – oznaczmy ją przez x.
   b. Wyliczamy liczbę elementów w poszczególnych płotkach.
   c. Dzielimy nasz kryptogram na płotki (o długości wyliczonej w poprzednim punkcie) i odczytujemy szukany tekst kolumnami.

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

## 5. Propozycje wykorzystania:

Jest wiele metod szyfrowania informacji. To zadanie można potraktować jako inspirację do wyszukiwania przez uczniów innych metod szyfrowania i zaprogramowania ich. Można klasę podzielić na grupy i każdej z grup przydzielić inną metodę. Jako zadanie dodatkowe można stworzyć program do deszyfrowania informacji zaszyfrowanej wyżej opisaną metodą.