WIT Szkoła Wyższa pod auspicjami Polskiej Akademii Nauk

Wydz. Informatyki WSISiZ

SPRAWDZIAN

Podstawy Programowania

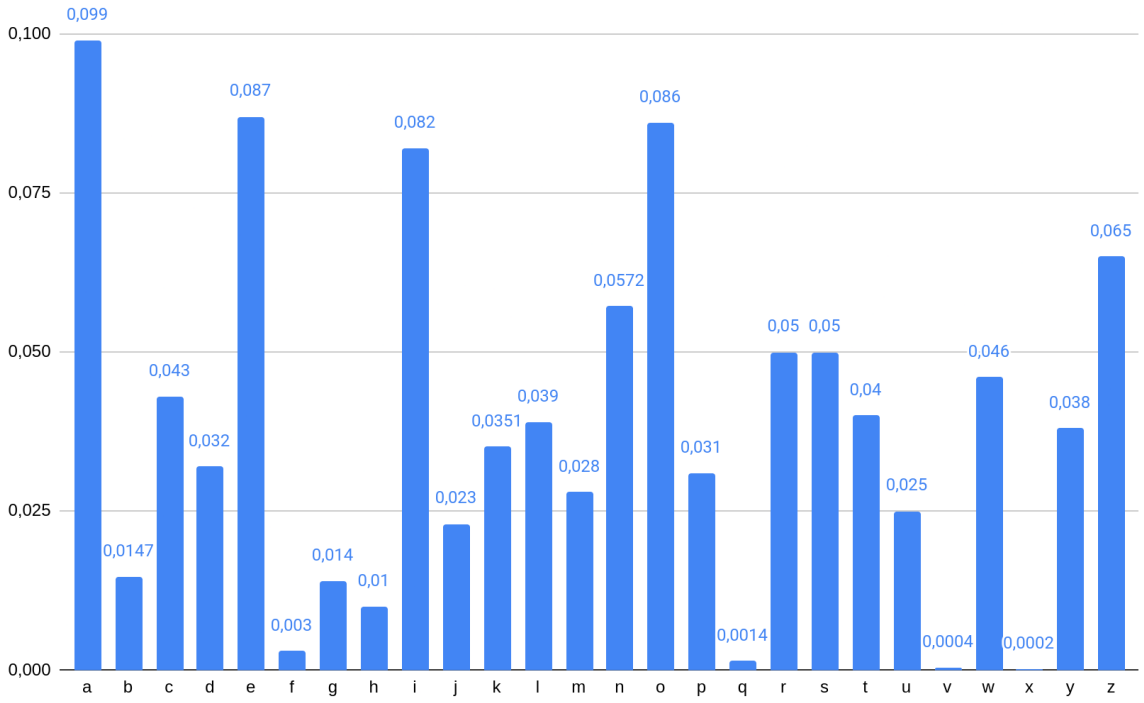
studia dzienne
grupa A02

Szyfrowanie z użyciem szyfru monoalfabetycznego polega na zamianie litery tekstu jawnego na dokładnie jedną literę w szyfrogramie. Są to bardzo proste szyfry możliwe do złamania bez używania żadnych urządzeń.

Jednym ze sposobów łamania takich szyfrów jest obliczenie rozkładu statystycznego dla szyfrogramu a następnie porównanie ich z rozkładem statystycznym dla języka w którym został napisany (lub poprzednich przechwyconych wiadomości). Porównaniu podlegają częstotliwości występowania danej litery w tekście. Znając że w języku polskim najczęściej używana litera jest ‘a’ oraz to że w szyfrogramie najczęściej występującą literą jest litera ‘g’ możemy przypuszczać że litery ‘a’ z tekstu jawnego zostały podmienione na literę ‘g’ w szyfrogramie.

Litery w języku polskim w kolejności od najczęściej występujących to:

a e o i z n s r w c l t y k d p m u j b g h f q v x



Napisz program umożliwiający użytkownikowi szyfrowanie, deszyfrowanie oraz łamanie szyfru. Stworzona aplikacja konsolowa przyjmuje 4 argumenty. Pierwszym argumentem jest nazwa polecenia "**enc**", "**dec**", "**btc**".
Dla polecenia "**enc**" program użyje reszty argumentów jako plik z słownikiem, kolejny argument użyje jako ścieżka do pliku wejściowego, Ostatnim będzie ścieżka do pliku wynikowego. Polecenie wczyta plik wejściowy, podstawi litery zgodnie ze słownikiem a następnie zapisze w pliku wynikowym.
Polecenie "**dec**" posiada takie same argumenty jednak dokonuje odszyfrowania pliku wejściowego.
Ostatnie wymagane polecenie to "**btc**" które w następnym argumencie przyjmuje ścieżkę do pliku z rozkładem przykładowym (przykład dla języka polskiego powyżej). Potem ścieżkę do pliku z badanym szyfrogramem. Czwartym argumentem programu jest ścieżka pod którą zapiszemy otrzymany słownik.

UWAGA! Słownik do szyfrowania i deszyfrowania jest identyczny. Różnica polega w zbudowanej funkcji.

W tym celu:

- ➔ Napisz funkcję ***encrypt*** przyjmująca stała referencje na słownik, oraz referencje na wektor ciągów znakowych. Funkcja dokonuje szyfrowanie tekstu jawnego według dostarczonego słownika modyfikując wektor ciągów znakowych.

- ➔ Napisz funkcję ***decrypt*** przyjmująca stała referencje na słownik, oraz referencje na wektor ciągów znakowych. Funkcja dokonuje deszyfrowania szyfrogramu według dostarczonego słownika modyfikując wektor ciągów znakowych.

- ➔ Napisz funkcję ***break_the_code*** przyjmująca stała referencje na rozkład statystyczny języka w którym jest stworzony szyfrogram, referencje na wektor ciągów znakowych, oraz referencje na wynikowy słownik. Zadaniem funkcji jest obliczenie rozkładu statystycznego badanego tekstu. Porównanie czestotliwosci wystepowania liter i stworzenie słownika do szyfrowania/deszyfrowania.

Słownik **można** zbudować jest jako ciąg liter w postaci:

```
std::string dict = "seoiznartclwykdpbujmghfqvx";
```

gdzie literę 'b' zamieniamy na 'e' co można zrealizować za pomocą:

```
char c = 'b';
dict[c - 'a']  // zwróci literę 'e'
```

Pamiętaj o sprawdzeniu liczby i poprawności argumentów. Oraz czy pliki zostały poprawnie otwarte. W razie problemów wyświetlić odpowiedni komunikat błędu.