

POLITECHNIKA ŚLĄSKA

WYDZIAŁ MATEMATYKI STOSOWANEJ

PROJEKT Z INFORMATYKI

Szyfrowanie Wiadomości

Student:
KAMIL KRÓL

2 STYCZNIA, 2018

Spis treści

| | | |
|----------|---------------------------------|----------|
| 1 | Opis programu | 1 |
| 2 | Instrukcja Obsługi | 2 |
| 3 | Techniczny Opis Programu | 3 |
| 3.1 | Biblioteki | 3 |
| 3.2 | Funkcja main() | 3 |
| 3.3 | Funkcje pomocnicze | 3 |
| 4 | Szczegóły techniczne | 4 |

1 Opis programu

Projekt jest rozwiązaniem zadania z konkursu Algorytmion 2015 - zadanie1 - "SZYFROWANIE WIADOMOŚCI".

Program ma za zadanie zaszyfrować wiadomość z pliku a następnie odszyfrować podaną wiadomość.

OPIS SZYFRU:

- Każdą literę i znak interpunkcyjny należy zamienić na odpowiadającą liczbę kodu ASCII (liczba naturalna od 0 do 127).
- Pierwsza, tak powstała liczba, jest zamieniana na system dwójkowy.
- Kolejne liczby, wynikające z kodu ASCII, są zamieniane na system liczbowy, który jest równy powiększonej o dwa reszcie z dzielenia przez osiem poprzedniej liczby.
- Ilość cyfr zamienionej liczby, dla każdego systemu liczbowego, wynika z ilości cyfr zamiany liczby maksymalnej, czyli liczby 127 (dla systemu binarnego jest to siedem cyfr).

KOLEJNOŚĆ WYKONYWANYCH DZIAŁAŃ PROGRAMU:

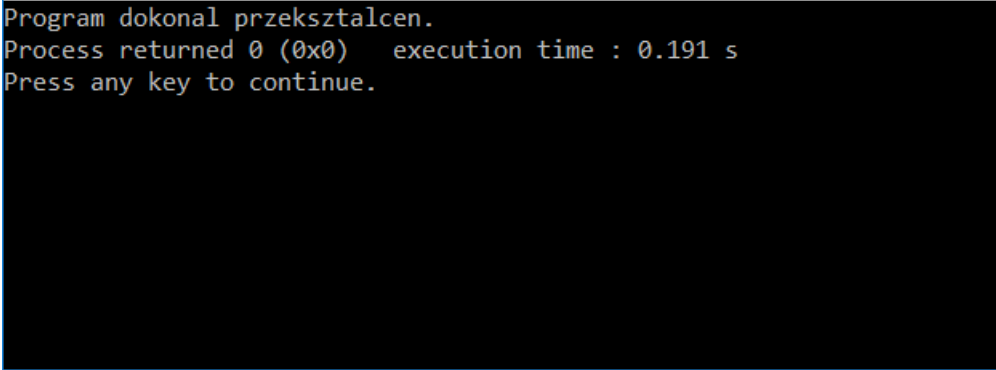
- Pobranie wiadomości z pliku text.txt (tylko pierwsza linijka)
- Szyfrowanie wiadomości
- Przesłanie kryptogramu do pliku szyfr.txt
- Odczyt kryptogramu z pliku szyfr.txt
- Odszyfrowanie wiadomości
- Wysłanie odszyfrowanej wiadomości do pliku odszyfrowane.txt

2 Instrukcja Obsługi

Do poprawnego działania programu wymagane jest utworzenie pliku szyfr.txt w folderze zawierającym program("projekt").

Do pliku szyfr.txt należy wprowadzić tylko jedną linię tekstu który życzymy sobie zaszyfrować.

Następnie należy uruchomić program który wyświetli w konsoli tylko jedną wiadomość:

A screenshot of a black console window with white text. The text reads: "Program dokonał przekształcen.", "Process returned 0 (0x0) execution time : 0.191 s", and "Press any key to continue.".

```
Program dokonał przekształcen.  
Process returned 0 (0x0) execution time : 0.191 s  
Press any key to continue.
```

Po zakończeniu działania programu zaszyfrowana wiadomość pojawi się w pliku szyfr.txt, zaś odszyfrowana w pliku odszyfrowanie.txt.

3 Techniczny Opis Programu

Program został napisany w języku C++ za pomocą IDE Code::Blocks oraz kompilatora GNU GCC Compiler.

3.1 Biblioteki

Do poprawnego działania programu zostały użyte trzy biblioteki.

- `iostream` - w celu wypisania wiadomości
- `fstream` - w celu możliwości pracy na plikach
- `string` - w celu wykorzystania funkcji działających na ciągach znaków takich jak `length()`

3.2 Funkcja `main()`

Funkcja `main` ma za zadanie odczyt danych z plików oraz wywołanie funkcji pomocniczych do szyfrowania jak i odszyfrowania wiadomości.

3.3 Funkcje pomocnicze

FUNKCJE SZYFRUJĄCE:

- `void szyfrowanie(string dane)`
funkcja szyfruje podany ciąg znaków oraz przesyła kryptogram do pliku
- `string usuniecie_spacji(string dane)`
funkcja usuwa spacje z podanego ciągu
- `string zamiana_systemu(char znak, int system)`
funkcja zamienia pojedynczy znak tekstu na szyfr w podanym systemie liczbowym

FUNKCJE DESZYFRUJĄCE:

- `void odszyfrowywanie(string dane)`
funkcja odszyfrowuje dany ciąg znaków i wysyła go do pliku
- `char odszyfrowanie_znaku(string znak, int system)`
funkcja odszyfrowuje pojedynczy znak

4 Szczegóły techniczne

Szyfrowanie danych polega na algorytmie symetrycznym, gdyż ten sam algorytm co szyfruje dane jest wykorzystywany do ich odszyfrowania.

Przykładowe szyfrowanie wiadomości "Ola".

| Znak | ASCII | System | Szyfr |
|------|-------|-------------------------|---------|
| O | 79 | 2 | 1001111 |
| l | 108 | $(79 \bmod 8) + 2 = 9$ | 130 |
| a | 97 | $(108 \bmod 8) + 2 = 6$ | 241 |

"O" posiada numer 79 w ASCII pierwszy znak szyfrujemy za pomocą systemu dwójkowego zatem $79_{(2)} = 1001111$.

"l" posiada numer 108 w ASCII. Żeby obliczyć kolejny system liczbowy do zaszyfrowania wykonujemy działanie $(\text{wcześniejszy znak}(\text{nr.ASCII}) \bmod 8) + 2 = \text{system}$.

Zatem $(79 \bmod 8) + 2 = 9$.

Teraz szyfrujemy znak za pomocą uzyskanego systemu liczbowego. $108_{(9)} = 130$.

Tak samo postępujemy z kolejnymi znakami aż do ich wyczerpania.

Stosując powyższy algorytm dla słowa "Ola" uzyskamy szyfr w postaci:

1001111 130 241

Odszyfrowywanie wygląda bardzo podobnie co szyfrowanie:

| Szyfr | System | ASCII(dziesiętny) | Znak |
|---------|-------------------------|-------------------|------|
| 1001111 | 2 | 79 | O |
| 130 | $(79 \bmod 8) + 2 = 9$ | 108 | l |
| 241 | $(108 \bmod 8) + 2 = 6$ | 97 | a |

Wiemy, że pierwszy znak jest zaszyfrowany w systemie dwójkowym zatem. $1001111_{(2)} = 79_{(10)}$.

Numer 79 w ASCII oznacza znak "O"

Żeby poznać w jakim systemie został zaszyfrowany kolejny znak stosujemy ten sam wzór co do szyfrowania:

$(\text{wcześniejszy znak}(\text{nr.ASCII}) \bmod 8) + 2 = \text{system}$.

Zatem $(79 \bmod 8) + 2 = 9$.

Po otrzymaniu systemu odszyfrowujemy znak. $130_{(9)} = 108_{(10)}$

Numer 108 w ASCII oznacza znak "l"

Tak samo postępujemy z kolejnymi zaszyfrowanymi znakami aż do ich wyczerpania.