Politechnika Śląska Wydział Matematyk Stosowanej Kierunek Informatyka

Gliwice, 24.01.2022

## Programowanie I

# projekt zaliczeniowy

"endeCRYPTION"

Bartosz Smolarz gr. lab. 2

### 1. Opis projektu.

Projekt ma za zadanie umożliwić użytkownikowi szyfrowanie oraz odszyfrowywanie (z kluczem) treści plików tekstowych.

#### 2. Wymagania

- -odszyfrowywanie pliku o rozszerzeniu .txt za pomocą klucza
- -szyfrowanie pliku o rozszerzeniu .txt za pomocą klucza

### 3. Przebieg realizacji

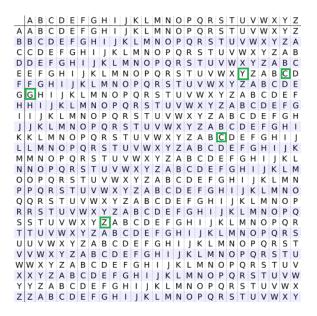
Projekt składa się z trzech plików:

- -endeCRYPTION.cpp (główny plik, zawierający wywołania funkcji)
- -funkcje.cpp (zawierający funkcje użyte do prawidłowego działania programu)
- -plik.h (zawierający deklaracje funkcji oraz ich opisy)

Zawartość plików została opisana w dokumentacji PDF, wygenerowanej przez Doxygen.

Do szyfrowania oraz odszyfrowywania z kluczem użyłem szyfru Vigenere'a. Jego działanie opisuję poniżej:

Tabela składa się z alfabetów wypisanych 26 razy w różnych rzędach, każdy alfabet przesuwany cyklicznie w lewo w stosunku do poprzedniego alfabetu, odpowiadający 26 możliwym szyfrom Cezara. W różnych punktach procesu szyfrowania szyfr używa innego alfabetu z jednego z wierszy. Alfabet użyty w każdym punkcie zależy od powtarzającego się słowa kluczowego.



Wejście: Tekst jawny: GEEKSFORGEEKS

Słowo kluczowe: AYUSZ

Wyjście: Tekst zaszyfrowany: GCYCZFMLYLEIM

W celu wygenerowania klucza podane słowo kluczowe jest powtarzane okrężnie, aż dopasuje długość do tekstu jawnego.

Słowo kluczowe "AYUSH" generuje klucz "AYUSHAYUSHAYU"

#### Szyfrowanie:

Pierwsza litera tekstu wejścia, G jest sparowana z A, pierwszą literą klucza. Używa się więc wiersza G i kolumny A kwadratu Vigenere'a, czyli G. Podobnie dla drugiej litery tekstu wejścia używana jest druga litera klucza, litera w rzędzie E, a kolumna Y to C. Reszta tekstu jawnego jest szyfrowana w podobny sposób.

## Odszyfrowywanie (z kluczem):

Odszyfrowanie odbywa się poprzez przejście do wiersza w tabeli odpowiadającego kluczowi, znalezienie pozycji litery tekstu zaszyfrowanego w tym wierszu, a następnie użycie etykiety kolumny jako tekstu jawnego. Na przykład w wierszu A (z AYUSH) zaszyfrowany tekst G pojawia się w kolumnie G, która jest pierwszą literą tekstu jawnego. Następnie przechodzimy do wiersza Y (z AYUSH), znajdujemy tekst zaszyfrowany C, który znajduje się w kolumnie E, stąd E jest drugą literą tekstu jawnego.

### 4. Instrukcja użytkownika

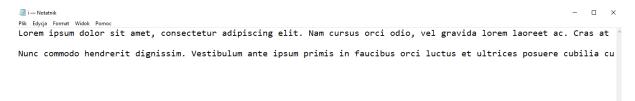


Po otwarciu pliku endeCRYPTION.cpp w wierszu poleceń wyświetlana jest instrukcja obsługi programu:

Aby zaszyfrować wpisz: -sz -nin nazwa\_wejścia.txt -nk nazwa\_klucza -nout nazwa\_wyjścia

Aby odszyfrować z kluczem wpisz: -od -nin nazwa\_wejścia.txt -nk nazwa\_klucza -nout nazwa wyjścia

Gdy wybierzemy opcję zaszyfrowania pliku (musimy mieć w folderze w którym uruchamiamy program potrzebne pliki tekstowe), a nasz plik wejścia nazywa się i.txt z zawartością:



Plik z kluczem nazywa się k.txt z zawartością:



Plik wyjścia nazywa się o.txt. to po wykonaniu komendy w wierszu poleceń:



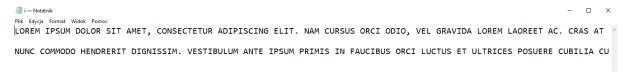
Plik wyjścia o.txt będzie zawierał zaszyfrowaną zawartość:

```
■ o - Notatnik
Pilk Edycja Format Widok Pomoc
UOEIW RPFYW MOYSB BIG EWNT, PSXBEPXOCUE ENRPVWMRNT IVRT. AEW LUEWEB OEGS XDVS, FNL TVKEIQE VXRRQ VJOEIOC AP. GBJS NX
AYXL CBQWXDB LOWDEIBRT QMQWIFWSV. VRWDRBHPEV AAXO RPFYW YRVQSB IA JKDCVFEB OEGS UUPXEB EG YVCRVGOB PBWENRR GEKIYMK LU
```

Gdy wybierzemy opcję odszyfrowania pliku postępujemy zgodnie z instrukcjami, jak w przykładzie z szyfrowaniem, z tą różnicą że wybieramy skrót -od, aniżeli -sz:



Plik wejścia i.txt będzie zawierał odszyfrowaną zawartość:



#### 5. Podsumowanie i wnioski.

W ramach programu zrealizowałem założone funkcje, odszyfrowywanie z kluczem oraz szyfrowanie. W niedalekiej przyszłości chcę usprawnić program o łączenie plików oraz odszyfrowywanie szyfrem Vigenere'a bez użycia klucza, metodą Kasiskiego.