

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.

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

Wejście: Tekst jawny: GEEKSFORGEEEKS

Słowo kluczowe: AYUSZ

Wyjście : Tekst zaszyfrowany : GCYZCFMLYLEIM

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):

4. Instrukcja użytkownika

[illegible]


Plik z kluczem nazywa się k.txt z zawartością:

janek

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

[illegible]

Plik wyjścia o.txt będzie zawierał zaszyfrowaną zawartość:



o - Notatnik

Plik Edycja Format Widok Pomoc


UOEIW RPFYW MOYSB BIG EWNT, PSXBEPXOCUE ENRPVWMRNT IVRT. AEW LUWEB OEGS XDVS, FNL TVKEIQE VXRRQ VJOEIOC AP. GBJS NX

AYXL CBQWXB LOWDEIBRT QMQWIFWSV. VRWDRBHEV 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:

[illegible]

Plik wejścia i.txt będzie zawierał odszyfrowaną zawartość:



The screenshot shows a standard Windows Notepad application. The title bar at the top reads "i — Notatnik". Below the title bar is a menu bar with the following items: "Plik", "Edycja", "Format", "Widok", and "Pomoc". The main text area contains two lines of Lorem Ipsum text: "LOREM IPSUM DOLOR SIT AMET, CONSECTETUR ADIPISCING ELIT. NAM CURSUS ORCI ODIO, VEL GRAVIDA LOREM LAOREET AC. CRAS AT" on the first line, and "NUNC COMMODO HENDRERIT DIGNISSIM. VESTIBULUM ANTE IPSUM PRIMIS IN FAUCIBUS ORCI LUCTUS ET ULTRICES POSUERE CUBILIA CU" on the second line. The text is in a monospaced font. The window has standard minimize, maximize, and close buttons in the top right corner.

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.