

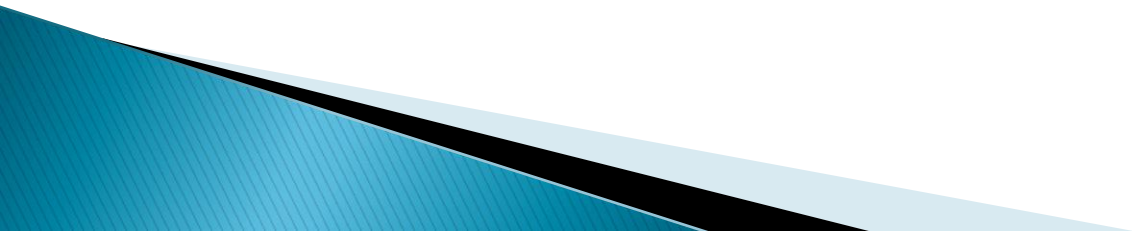
Języki Asemblerowe – projekt

Szyfrowanie plików algorytmem Vigenère

Patryk Gregorczyk



Plan prezentacji

- ▶ Kim był Vigenere?
 - ▶ Kto wymyślił szyfr Vigenere?
 - ▶ Do czego służy i jak działa algorytm?
 - ▶ Krótki opis programu i wyglądu GUI
- 

Blaise de Vigenère

- ▶ Francuski kryptograf, dyplomata i alchemik.
- ▶ Żył w XVI wieku.
- ▶ Autor zmodyfikowanego szyfru Vigenere.



Historyczny błąd

Szyfr znany dzisiaj jako szyfr Vigenere, został po raz pierwszy opisany przez Giovana Batista Belaso w 1553r.

W XIX wieku wynalezienie to zostało błędnie przypisane Vigenerowi, przez co dzisiaj nosi nazwę szyfru Vigenere.

Vigenere był autorem jego zmodyfikowanej wersji opartej o szyfrowanie za pomocą tzw. autoklucza.



Szyfr Vigenere

- ▶ Polialfabetyczny szyfr podstawieniowy
- ▶ Szyfr w wersji historycznej wymaga klucza (Belasso)
- ▶ Wersja oryginalna korzysta z autoklucza (Vigenere)

Tablica szyfrująca

Kolejne wiersze są przesunięte względem poprzedniego o jeden w lewo, a „wypadające” litery wracają w tej samej kolejności z prawej strony.

Tablice można dowolnie zmodyfikować dodając np. litery ze znakami diakrytycznymi dostosowując go do potrzeb danego języka.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Sposób szyfrowania

- ▶ Szyfrujemy wiadomość np. „SMIW I ASEMBLER”
- ▶ Podajemy klucz np. „ECTSY”
- ▶ Odczytujemy kolejne litery z tablicy szyfrującej.
(W wersji z autokluczem ustala się tylko pierwszą literę klucza, a kolejne są poprzednimi literami szyfrowanego tekstu.)

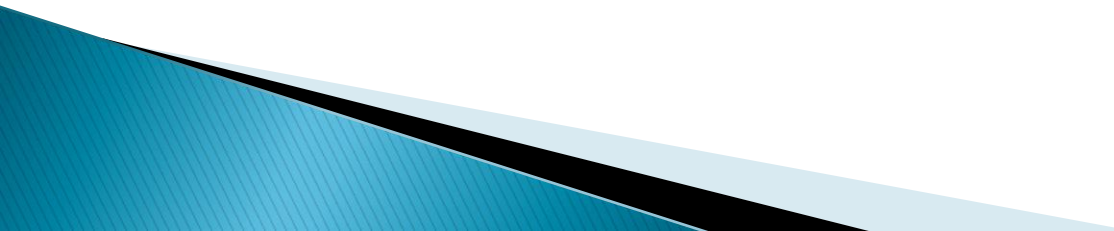
Pierwsza będzie ta która znajduje się na przecięciu wiersza ‘S’ z kolumną ‘E’, czyli ‘W’.

Druga litera: wiersz ‘M’ z kolumną ‘C’ otrzymujemy ‘O’.

Szyfrowanie trzeciej
liter 'I' za pomocą
liter 'T'.
Otrzymujemy 'B'.


	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

Wiadomość: SMIW I ASEMBLER
Klucz ECTSYECTSYECTSY
Zaszyfrowana wiadomość: WOBO M TKCQDEWR



Ciekawostka

W 1949r. Udowodniono, że szyfr ten jest szyfrem nie do złamania, o ile zachowane zostaną następujące reguły:

- ▶ klucz użyty do szyfrowania wiadomości musi być dłuższy lub równy szyfrowanej wiadomości;
 - ▶ klucz musi być wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych);
 - ▶ klucz nie może być użyty do zaszyfrowania więcej niż jednej wiadomości;
 - ▶ dodatkowo jest wymagane, aby osoba znająca klucz nikomu go nie zdradziła.
- 

Implementacja

- ▶ Program główny napisany w C# z wykorzystaniem Windows Presentation Foundation (WPF).
- ▶ Biblioteki w języku C++ oraz asemblerze każda z dwoma funkcjami: szyfrującą i deszyfrującą.
- ▶ Obsługa wielowątkowości poprzez metodę ForEach z klasy Parallel.
- ▶ Aplikacja szyfruje jeden wskazany plik i zapisuje do wskazanego folderu (domyślnie ten sam co plik wejściowy) z dopisanym do nazwy suffixem „_res”.
- ▶ Możliwość ustawienia rozmiaru bufora do którego pobierane są dane z pliku na 1MB, 2MB, 4MB lub 8MB (np. dla testów).

Interfejs graficzny

Vigenere Coding

Input file: ...

Output file: ...

Cipher key:

Threads: 1

Choose library:

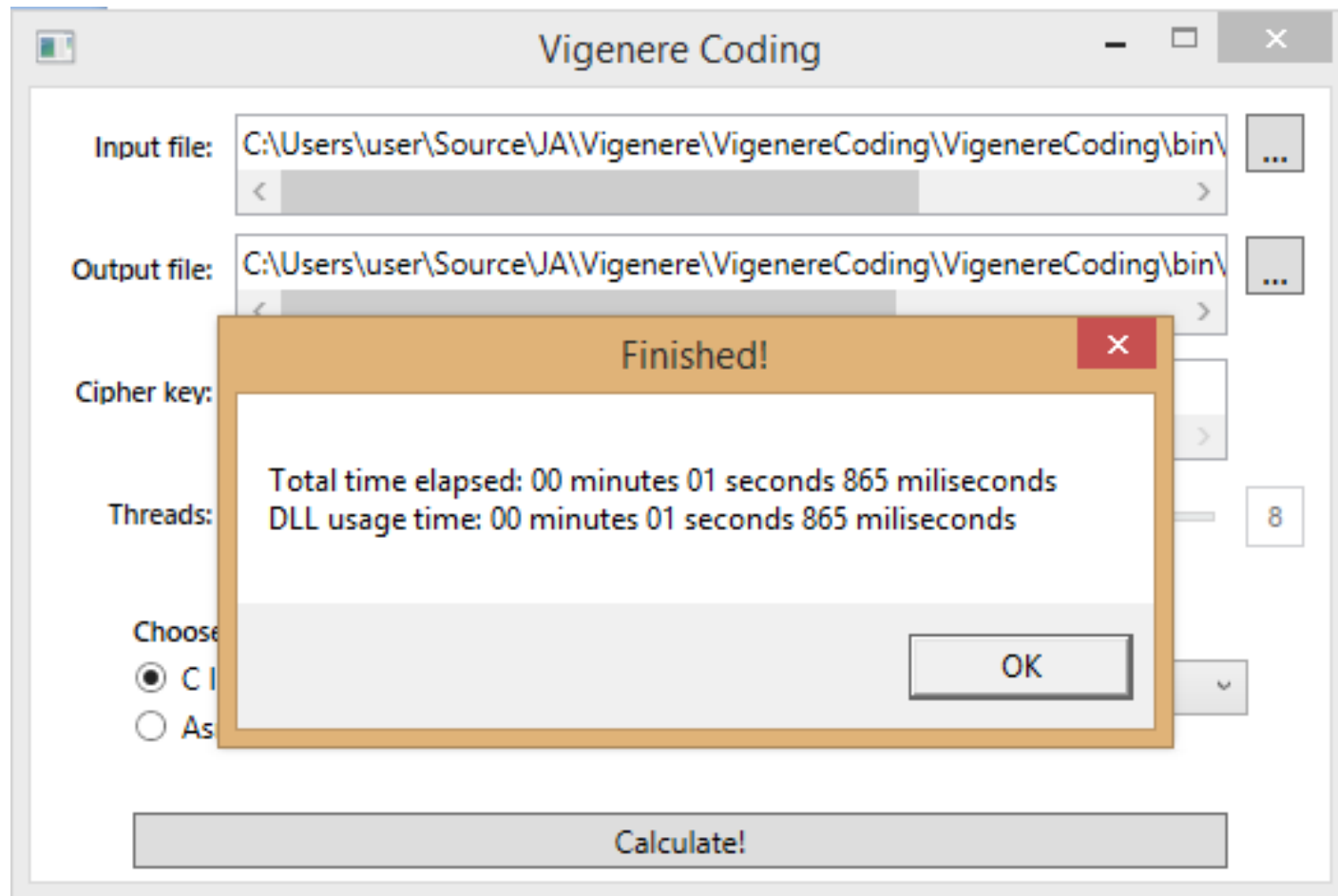
- ☐ C library
- ☐ Asm library

Choose mode:

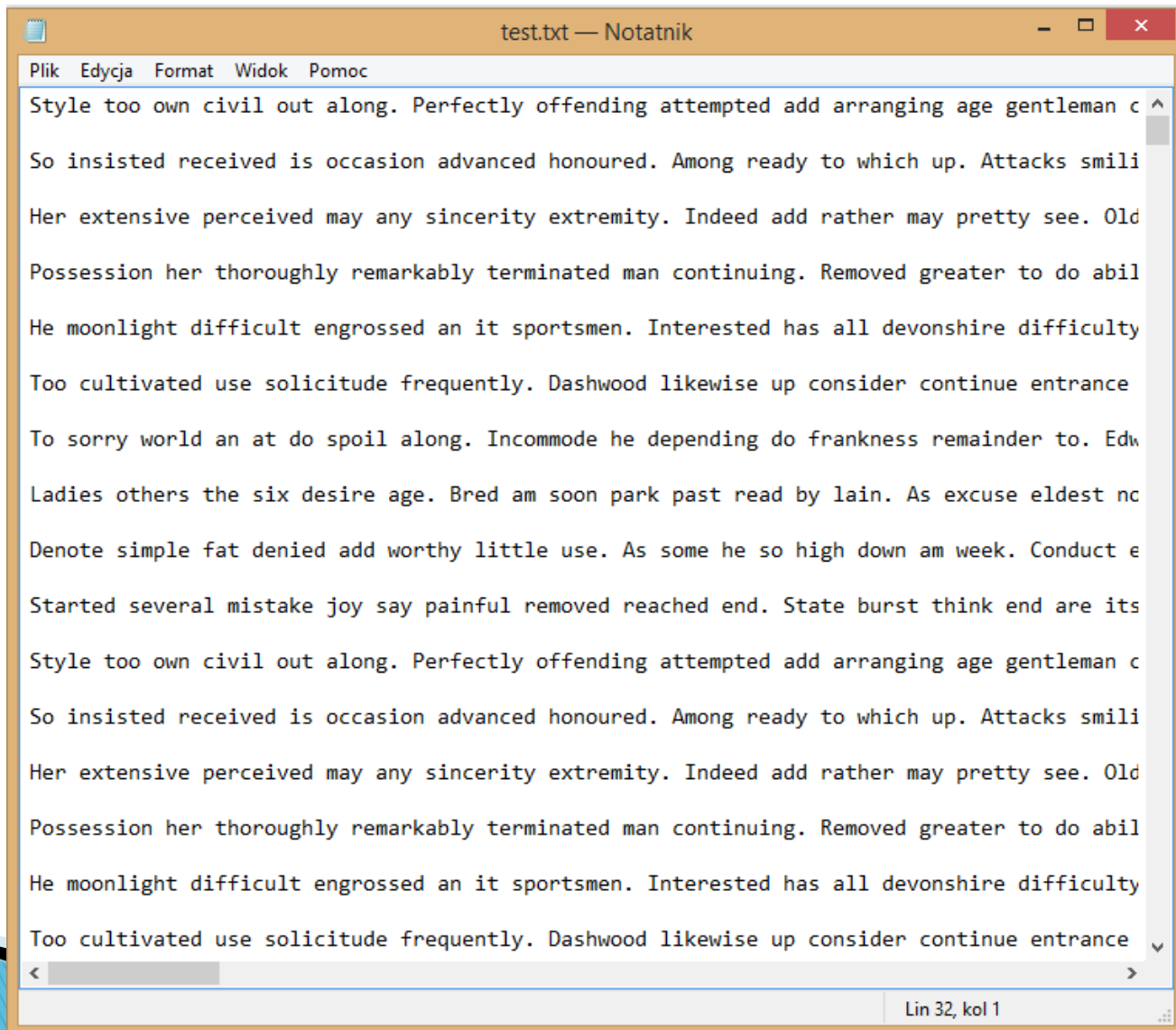
- ☐ Coding
- ☐ Decoding

Buffer size [B]: 4096

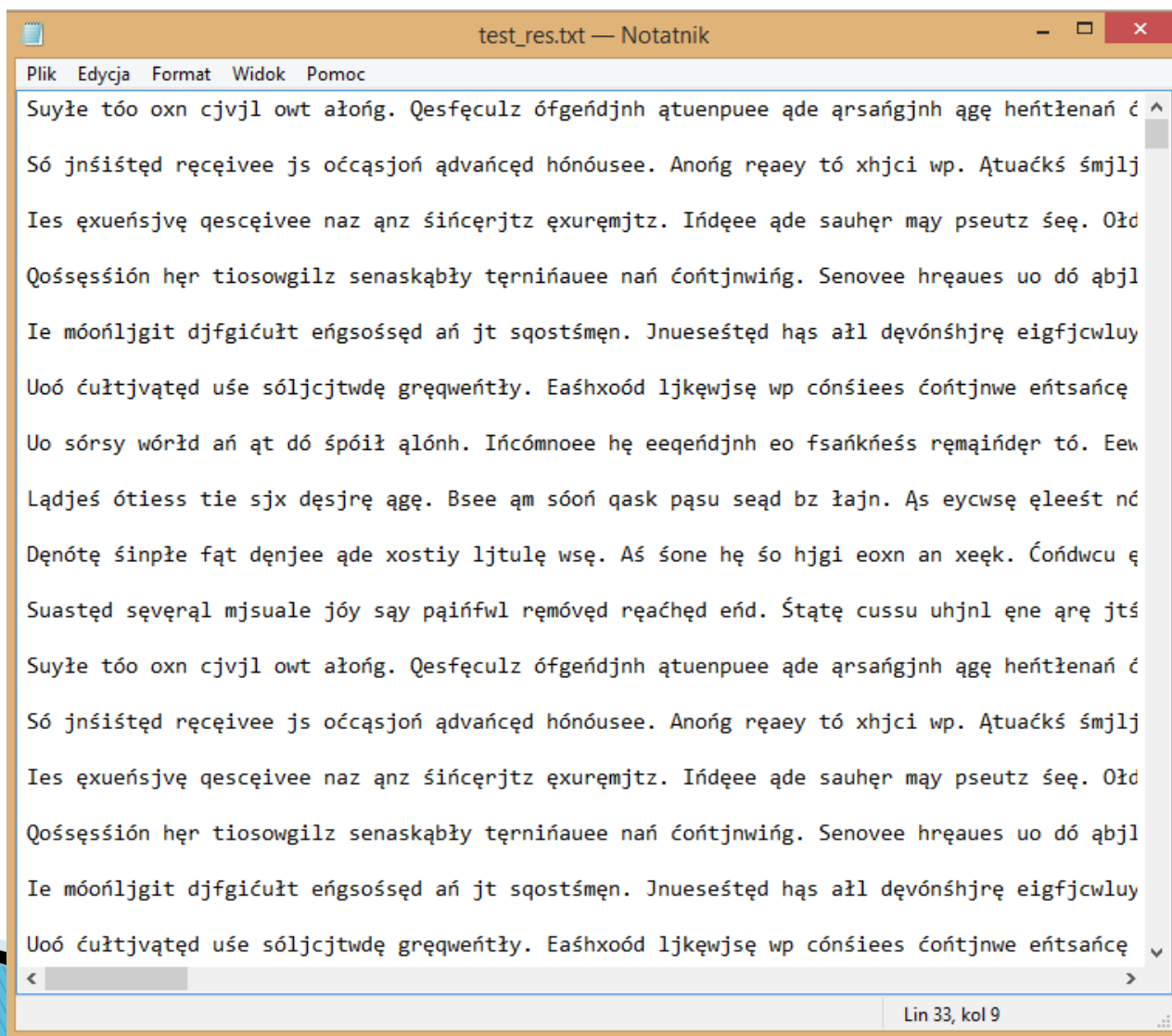
Calculate!



Plik wejściowy:



Plik wynikowy po zaszyfrowaniu kluczem „AA” (co druga litera przesunięta o 1).



Dziękuję za uwagę.