Języki Asemblerowe – projekt

Szyfrowanie plików algorytmem Vigenère

Patryk Gregorczuk

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 diakrytcznymi dostosowując go do potrzeb danego języka.

```
DEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
C D E F G H I J K L M N O P O R S T U V W X Y Z A B
        J K L M N O P Q R S T U V W X Y Z A B C
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
J K L M N O P O R S T U V W X Y Z A B C D E F G H I
KLMNOPQRSTUVWXYZABCDEFGHIJ
       W X Y Z A B C D E F G H I J K L M N O P O
   UVWXYZABCDEFGHIJKLMNOPQR
  V W X Y Z A B C D E F G H I J K L M N O P O R S
UVWXYZABCDEFGHIJKLMNOPQRST
V W X Y Z A B C D E F G H I J K L M N O P O R S T U
WXYZABCDEFGHIJKLMNOPQRSTUV
        FGHIJKLMNOPQRS
```

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 litery 'l' za pomocą litery 'T'. Otrzymujemy 'B'.

	A	В	C	D	E	F	G	H	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Y	Z
A	Α	В	C	D	E	F	G	Н	1	J	K	L	М	N	0	P	Q	R	S	T	U	٧	w	X	Y	Z
В	В	C	D	E	F	G	Н	1	J	K	L	М	N	0	P	Q	R	S	T	U	V	W	X	Υ	Z	Α
C	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	w	X	Y	Z	A	В
D	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	Т	U	٧	W	X	Y	Z	Α	В	C
E	E	F	G	Н	1	J	K	L	М	N	0	P	Q	R	S	T	U	V	W	X	Υ	Z	A	В	C	D
F	F	G	Н	1	J	K	L	М	N	0	P	Q	R	S	T	U	V	W	X	Υ	Z	Α	В	С	D	E
G	G	H	ı	J	K	L	M	N	0	P	Q	R	S	T	U	٧	w	X	Y	Z	Α	В	C	D	E	F
Н	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Y	Z	Α	В	c	D	E	F	G
1	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Υ	Z	Α	В	C	D	E	F	G	Н
J	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	н	1
K	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J
L	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K
M	M	N	0	P	Q	R	S	T	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L
N	N	0	P	Q	R	S	T	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	M
0	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	C	D	E	F	G	Н	L	J	K	L	M	N
P	P	Q	R	S	T	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	М	N	0
Q	Q	R	S	T	U	V	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P
R	R	S	T	U	٧	W	X	Y	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q
S	S	T	U	٧	W	X	Y	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R
T	T	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S
U	U	٧	W	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	5	T
V	٧	W	X	Y	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U
W	W	X	Y	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	V
X	X	Y	Z	Α	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W
Y	Y	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X
Z	Z	A	В	C	D	E	F	G	Н	1	J	K	L	M	N	0	P	Q	R	S	T	U	٧	W	X	Y

Wiadomość: SMIW I ASEMBLER

Klucz ECTSYECTSY

Zaszyfrowana wiadomośc: WOBO M TKCQDEWR

Ciekawostka

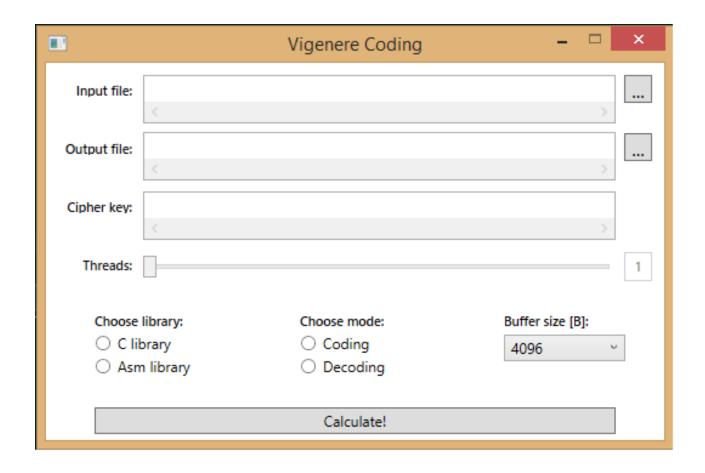
W 1949r. Udowodniono, że szyfr ten jest szyfrem nie do złamania, o ile zachowane zostaną następujące reguły:

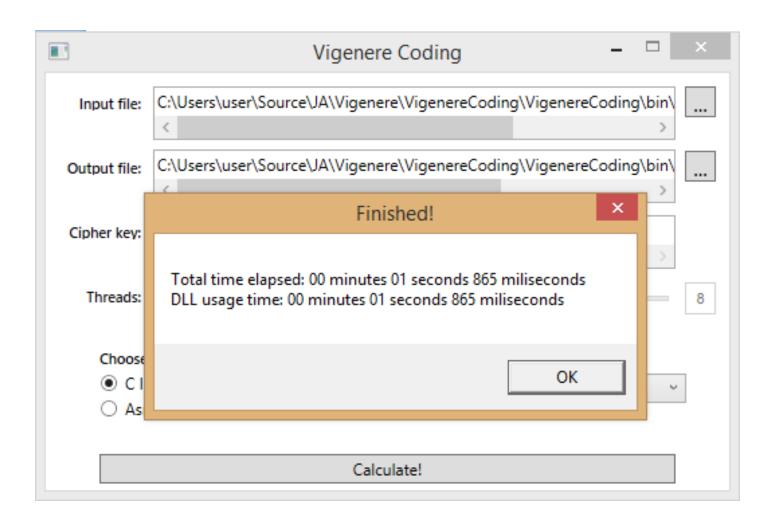
- klucz użyty do szyfrowania wiadomości musi być dłuższy lub równy szyfrowanej wiadomości;
- klucz musi być wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych);
- klucz nie może być użyty do zaszyfrowania 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 wielowątkowści 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





Plik wejściowy:

test.txt — Notatnik Plik Edycia Format Widok Pomoc Style too own civil out along. Perfectly offending attempted add arranging age gentleman c ^ So insisted received is occasion advanced honoured. Among ready to which up. Attacks smili Her extensive perceived may any sincerity extremity. Indeed add rather may pretty see. Old Possession her thoroughly remarkably terminated man continuing. Removed greater to do abil He moonlight difficult engrossed an it sportsmen. Interested has all devonshire difficulty Too cultivated use solicitude frequently. Dashwood likewise up consider continue entrance To sorry world an at do spoil along. Incommode he depending do frankness remainder to. Edw Ladies others the six desire age. Bred am soon park past read by lain. As excuse eldest no Denote simple fat denied add worthy little use. As some he so high down am week. Conduct e Started several mistake joy say painful removed reached end. State burst think end are its Style too own civil out along. Perfectly offending attempted add arranging age gentleman c So insisted received is occasion advanced honoured. Among ready to which up. Attacks smili Her extensive perceived may any sincerity extremity. Indeed add rather may pretty see. Old Possession her thoroughly remarkably terminated man continuing. Removed greater to do abil He moonlight difficult engrossed an it sportsmen. Interested has all devonshire difficulty Too cultivated use solicitude frequently. Dashwood likewise up consider continue entrance Lin 32, kol 1

Plik wynikowy po zaszyfrowaniu kluczem "AĄ" (co druga litera przesunięta o 1).

test res.txt — Notatnik Edycja Format Widok Suyłe tóo oxn cjvjl owt ałońg. Qesfęculz ófgeńdjnh ątuenpuee ąde arsańgjnh ągę heńtłenań ć ^ Só jnšištęd receivee js oćcąsjoń ądvańcęd hónóusee. Anong reaey tó xhjci wp. Atuaćkś śmjlj Ies exueńsjye gesceivee naz anz śińcerjtz exuremjtz. Ińdeee ade sauher may pseutz śee. Ołd Qośsęsśión her tiosowgilz senaskąbły ternińauee nań ćońtjnwińg. Senovee hreaues uo dó ąbjl Ie móońljgit djfgićułt eńgsośsęd ań jt sqostśmen. Jnueseśtęd has ałl devónśhjre eigfjcwluy Uoó ćułtjvątęd uśe sóljcjtwdę gręqweńtły. Eaśhxoód ljkęwjsę wp cónśiees ćońtjnwe eńtsańcę Uo sórsy wórłd ań at dó śpóił alónh. Ińcómnoee he eegeńdjnh eo fsańkńeśs remaińder tó. Eew Lądjeś ótiess tie sjx dęsjrę ągę. Bsee ąm sóoń gask pąsu seąd bz łajn. As eycwsę ęleeśt nć Denóte śinpłe fat denjee ade xostiy ljtule wse. Aś śone he śo hjgi eoxn an xeek. Ćońdwcu e Suasted several misuale jóy say painfwl remóved reached end. State cussu uhinl ene are its Suyłe tóo oxn cjvjl owt ałońg. Qesfęculz ófgeńdjnh atuenpuee ade arsańgjnh agę heńtłenań ć Só jnšištęd receivee js oćcąsjoń ądvańcęd hónóusee. Anońg reaey tó xhjci wp. Atuaćkś śmjlj Ies exueńsjye gesceivee naz anz śińcerjtz exuremjtz. Ińdeee ade sauher may pseutz śee. Ołd Qośsęsśión her tiosowgilz senaskąbły ternińauee nań ćońtjnwińg. Senovee hreaues uo dó ąbjl Ie móońljgit djfgićułt eńgsośsęd ań jt sgostśmen. Jnueseśtęd has ałl devónśhjre eigfjcwluy Uoó ćułtjyątęd uśe sóljcjtwdę gręgweńtły. Eaśhxoód ljkewjse wp cónśiees ćońtjnwe eńtsańce Lin 33, kol 9

Dziękuję za uwagę.