Zaprojektowanie i implementacja aplikacji szyfrująco-deszyfrującej wiadomości

Kryptografia 2
Projekt

Hubert Droździak

Politechnika Wrocławska 2021

1 Wstęp

1.1 Kryptografia

Kryptografia, jest jedną z odnóg kryptologii, zajmuje się utajnianiem informacji. Za najważniejsze zastosowania kryptologii uznaje się utajnianie informacji w wojskowości i dyplomacji. W tych zastosowaniach używa się najbardziej zaawansowanych funkcji i protokołów kryptograficznych. Współcześnie kryptografia jest uznawana za gałąź zarówno matematyki, jak i informatyki.

1.2 Cel projektu

Projekt polega na stworzeniu aplikacji szyfrująco- deszyfrującej, która ma za zadanie w miarę prosty sposób utajniać rozmowy np. mailowe, sms-owe. System nie może być implementacją wprost już istniejących metod kryptograficznych.

1.3 Użyty język i środowisko programistyczne

Do implementacji aplikacji, użyty został język C++ w środowisku Code::Blocks.

1.4 Zaimplementowane biblioteki

- iostream
- conio.h
- ctime
- vector
- cstdlib

1.5 Zmienne globalne

- const int rozmiar - rozmiar tablicy znaków
- const char znaki[rozmiar] - stworzona tablica znaków
- vector <char> ostatnioSzyfrowane - odpowiada za zapamiętnie ostatnio stworzonego szyfru
- int ostatniDzien, ostatniMiesiac, ostatniRok - w tych zmiennych zapamiętywana jest data stworzenia ostatnio stworzonego szyfru

1.6 Funkcje w aplikacji

- void strToDate(string tekst, int &d, int &m, int &r) - funkcja zamienia otrzymany string na dzien, miesiac i rok
- void pobierzDate(int &d, int &m, int &y) - funkcja odpowiada ze pobieranie daty z urządzenia.
- int dodawanieModulo(int a, int b) - funkcja zwraca sumę modulo dwóch liczb
- int odejmowanieModulo(int a, int b) - funkcja zwraca różnicę modulo dwóch liczb
- int mnozenieModulo(int a, int b) - funkcja zwraca iloczyn modulo dwóch liczb
- int dzielenieModulo(int a, int b) - funkcja zwraca iloraz modulo dwóch liczb
- void zapiszSzyfr(vector <char> szyfr, int d, int m, int r) - funkcja zapisuje do zmiennych globalnych szyfr, dzień, miesiąc i rok. W przypadku kiedy już coś znajdowało się w tablicy, to najpierw jest czyszczona.
- void wczytajSzyfr(vector <int> &szyfrLiczby, int &d, int &m, int &r) - funkcja wczytuje dane ze zmiennych globalnych do argumentów, kiedy jest już zapisany szyfr.
- void szyfrowanie() - jedna z głównych funkcji programu, w tej funkcji wpisujemy tekst jawny i otrzymujemy zaszyfrowaną wiadomość.
- void deszyfrowanie() - jedna z głównych funkcji programu, w tej funkcji wpisujemy szyfr oraz datę i otrzymujemy odszyfrowaną wiadomość.
- void wyswietlMenu() - funkcja wyświetla menu główne

2 Działanie aplikacji

Fundamentalnym elementem aplikacji jest wykorzystywana standardowa tablica znaków, wygląda ona tak:

A	a	B	b	C	c	D	d	E	e	F	f	G	g
H	h	I	i	J	j	K	k	L	l	M	m	N	n
O	o	P	p	Q	q	R	r	S	s	T	t	U	u
V	v	W	w	X	x	Y	y	Z	z	1	2	3	4
5	6	7	8	9	0	(spacja)	,	.	?	!	’	”	;
:	/	\	—	-	_	+	=	<	>	(	)	*	&
^	%	$	#	@	[	]	{	}	~	‘	♥	☺	

W tablicy znajduje się 97 znaków tablicy ASCII, względem tej liczby wyznaczana jest reszta modulo. Dwa ostatnie znaki mogą zostać otrzymane odpowiednio naciskając kombinację klawiszy: alt+3 (♥) oraz alt+1 (☺).

2.1 Szyfrowanie

Szyfrowanie przebiega w 6 etapach:

1. Najpierw tablica znaków jest mieszana, za pomocą generatora liczb pseudolosowych, o ziarnie składającym się z aktualnej daty (dzień, miesiąc, rok) oraz długości tekstu jawnego.
2. Następnie każda litera jest zamieniana na liczbę, odpowiadającą miejscu, w przemieszanej już, tabeli.
3. W dalszej kolejności każda kolejna liczba jest sumą modulo siebie i dwóch poprzednich, począwszy od drugiej liczby.
4. Wykonywana jest suma modulo wszystkich liczb pomnożonych przez numer w tabeli.
5. Wykonana suma jest następnie dodawana do każdej z liczb osobno.
6. Na koniec liczby są zamieniane w znaki za pomocą standardowej tablicy. Taki szyfr jest gotowy do wysłania.

2.2 Deszyfrowanie

Etapy deszyfrowania:

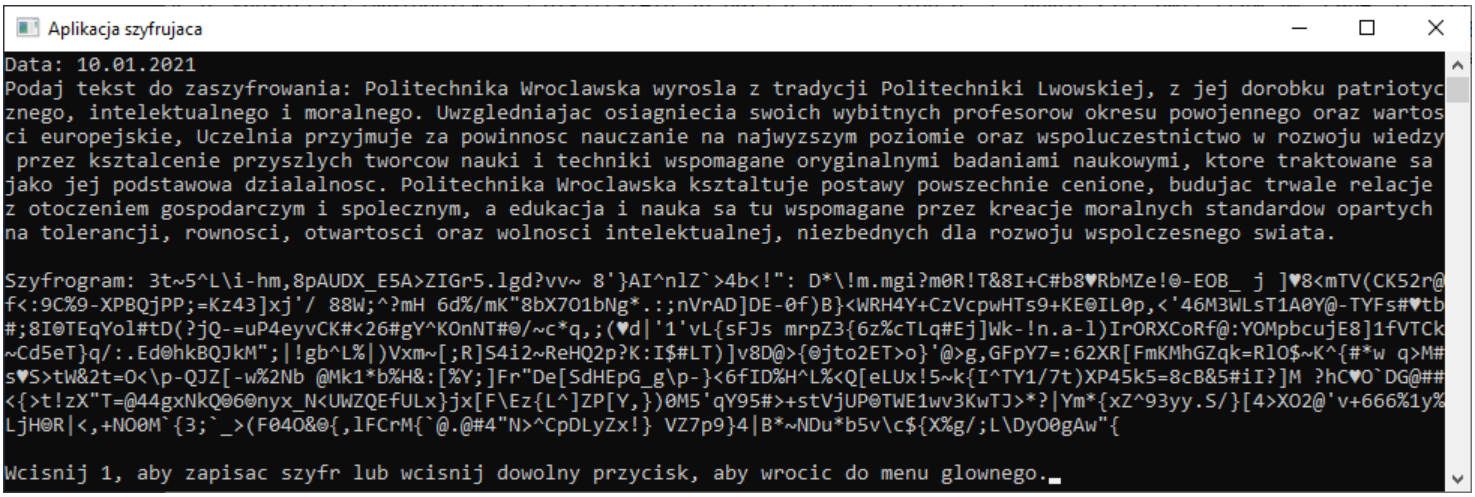
1. Szyfr jest zamieniany na liczby, odpowiadające numerowi miejsca w standardowej tablicy znaków.
2. Wykonywana jest suma modulo wszystkich liczb pomnożonych przez numer w tabeli, która następnie jest dzielona modulo przez sumę modulo kolejnych numerów miejsc liczb w tablicy na końcu powiększonych o $\underline{1}$. (np. dla szyfru o długości 4 to mianownik dzielenia modulo wynosi 7 (0+1+2+3+$\underline{1}$=7)).
3. Wykonana wyżej suma jest odejmowana modulo od każdej z liczb w tablicy.
4. Zaczynając od ostatniej liczby w tablicy liczb, odejmowane modulo są od niego dwie wcześniejsze liczby, aż do drugiej liczby w tablicy.
5. Na sam koniec tablica znaków jest mieszana za pomocą tego samego ziarna jakim została pomieszana podczas szyfrowania.
6. Ostatnim krokiem jest zmiana liczb na znaki, jako że liczby oznaczają numer w przemieszanej tablicy znaków. Odszyfrowana wiadomość jest gotowa do wyświetlenia.

3 Przykład użycia

3.1 Tekst jawny

Politechnika Wroclawska wyrosla z tradycji Politechniki Lwowskiej, z jej dorobku patriotycznego, intelektualnego i moralnego. Uwzgledniajac osiagniecia swoich wybitnych profesorow okresu powojennego oraz wartosci europejskie, Uczelnia przyjmuje za powinnosc nauczanie na najwyzszym poziomie oraz wspoluczestnictwo w rozwoju wiedzy przez ksztalcenie przyszlych tworcow nauki i techniki wspomagane oryginalnymi badaniami naukowymi, ktore traktowane sa jako jej podstawowa dzialalnosc. Politechnika Wroclawska ksztaltuje postawy powszechnie cenione, budujac trwale relacje z otoczeniem gospodarczym i spolecznym, a edukacja i nauka sa tu wspomagane przez kreacje moralnych standardow opartych na tolerancji, rownosci, otwartosci oraz wolnosci intelektualnej, niezbednych dla rozwoju wspolczesnego swiata.

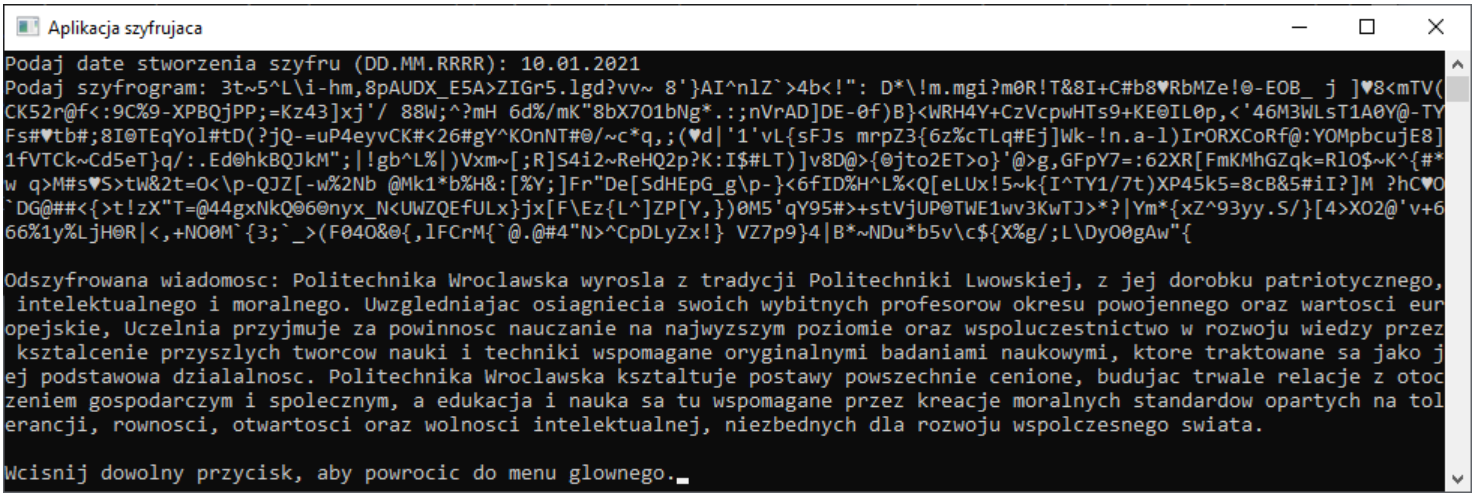
3.2 Szyfrowanie



3.3 Otrzymany szyfr

```
3t~5^L\i-hm,8pAUDX_E5A>ZIGr5.lgd?vv~ 8'}AI^nlZ`>4b<!": D*\!m.mgi?m0R!T&8I+C#b8♥RbMZe!@-EOB_ j ]♥8<mTV(CK52r@f<:9C%9-XPBQjPP;=Kz43]xj'/
88W;^?mH 6d%/mK"8bX7O1bNg*.:;nVrAD]DE-0f)B}<WRH4Y+CzVcpwHTs9+KE@IL0p,<'46M3WLsT1A0Y@-TYFs#♥tb#;8I@TEqYol#tD(?jQ-=uP4eyvCK#<26#gY^KOnNT#
@/~c*q,;(♥d|'1'vL{sFJs mrpZ3{6z%cTLq#Ej]Wk-!n.a-l)IrORXCoRf@:YOMpbcujE8]1fVTCk~Cd5eT}q/:.Ed@hkBQJkM";|!gb^L%|)Vxm~[;R]S4i2~ReHQ2p?K:I
$#LT)]v8D@>{@jto2ET>o}'@>g,GFpY7=:62XR[FmKMhGZqk=RlO$~K^{#*w q>M#s♥S>tW&2t=O<\p-QJZ[-w%2Nb @Mk1*b%H&:[%Y;]Fr"De[SdHEpG_g\p-}<6fID%H^L%<Q
[eLUx!5~k{I^TY1/7t)XP45k5=8cB&5#iI?]M ?hC♥O`DG@##<{>t!zX"T=@44gxNkQ@6@nyx_N<UWZQEfULx}jx[F\Ez{L^]ZP[Y,})0M5'qY95#>+stVjUP@TWE1wv3KwTJ>*?|Ym*
{xZ^93yy.S/}[4>XO2@'v+666%1y%LjH@R|<,+NO0M`{3;`_>(F04O&@{,lFCrM{`@.@#4"N>^CpDLyZx!} VZ7p9}4|B*~NDu*b5v\c${X%g/;L\DyO0gAw"{
```

3.4 Deszyfrowanie



4 Podsumowanie

Program działa w sposób dobry, jest w stanie zaszyfrować dość długie wiadomości.

Jednym z plusów jest to, że nawet kiedy ktoś będzie znał sposób deszyfrowania, to jeżeli nie ma całego szyfrogramu, bądź szyfrogram będzie mieć podmieniony choć jeden znak, to osoba postronna nie będzie w stanie odszyfrować wiadomości.

Jednym z minusów jest zastosowana tablica, nie uwzględnia specjalnych liter z języka polskiego tj. ą, ę, ć, ś, ó, ź, ż, ń, ł. Aczkolwiek trzeba pamiętać, iż jest to prosty program o małym stopniu zaawansowania.