Министерство образования и науки

Республики Казахстан

Карагандинский государственный технический университет

Кафедра

**КУРСОВАЯ РАБОТА**

на тему: Текстовый редактор "Блокнот" с функцией шифрования -

дешифрования классическими криптографическими методами

**Выполнил:**

**Проверил:**

**Караганда 2009 г.**

Содержание

Введение

Теоретическая часть

Шифры простой замены

Гаммирование

Шифры перестановки

Двойная перестановка столбцов и строк

Метод шифрования с использованием таблицы Виженера

Практическая часть

Вывод

Листинг программы

## Введение

**Цель работы:**

Изучение принципа программной реализации классических криптографических методов:

метод Цезаря;

метод Гронсфельда;

метод гаммирования;

метод двойных перестановок;

метод замены с использованием таблицы Виженера.

**Задание:**

1. Необходимо создать текстовый редактор "Блокнот", который содержал следующие объекты:

окно ввода исходного текста;

окно вывода зашифрованного текста;

кнопки "Шифровать", "Дешифровать", "Выбор метода шифрования";

строка меню, содержащая меню для работы с файлами, меню для работы с текстом (вырезать, вставить, отменить, повторить, поиск и т.д.), меню для выбора методов шифрования, меню "о программе" и "о разработчике".

Составить вербальный алгоритм для каждого метода шифрования.

Составить программу для шифрования заданными методами.

Составить программу для дешифрования заданными методами.

Оценить результативность реализованных методов.

## Теоретическая часть

## Шифры простой замены

**Система шифрования Цезаря** - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

**Шифры сложной замены**

**Шифр Гронсфельда** состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр - 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

|  |  |
| --- | --- |
|  | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| А | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_ |
| Б | \_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ |
| В | Я\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ |
| Г | ЮЯ\_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ |
| . | ………… |
| Я | ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_АБ |
| \_ | БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ\_А |

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

|  |  |
| --- | --- |
| Сообщение | ПРИЕЗЖАЮ\_ШЕСТОГО |
| Ключ | АГАВААГАВААГАВАА |
| Шифровка | ПНИГЗЖЮЮЮАЕОТМГО |

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

## Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки Т (0) i одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков Г (ш) i аналогичной длины (Т (ш) i=Г (ш) i+Т (0) i, где + - побитовое сложение, i =1-m).

Процесс дешифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные T (0) i=Г (ш) i+Т (ш) i.

## Шифры перестановки

**Алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2 | 4 | 1 | 3 |  |  | 1 | 2 | 3 | 4 |  |  | 1 | 2 | 3 | 4 |
| 4 | П | Р | И | Е |  | 4 | И | П | Е | Р |  | 1 | А | З | Ю | Ж |
| 1 | З | Ж | А | Ю |  | 1 | А | 3 | Ю | Ж |  | 2 | Е | \_ | С | Ш |
| 2 | \_ | Ш | Е | С |  | 2 | Е. | \_ | С | Ш |  | 3 | Г | Т | О | О |
| 3 | Т | О | Г | О |  | 3 | Г | Т | О | О |  | 4 | И | П | Е | Р |

## Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ\_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5\*5 их 14400.

## Метод шифрования с использованием таблицы Виженера

Этот шифр можно описать таблицей шифрования, называемой таблицей Виженера, по имени Блеза Виженера, дипломата XVI века, который развивал и совершенствовал криптографические системы:

|  |  |
| --- | --- |
|  | АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ |
| А | АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ |
| Б | \_АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ |
| В | Я\_АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮ |
| Г | ЮЯ\_АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭ |
|  | ... ... |
| Я | ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ\_АБ |
| \_ | БВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ\_А |

Каждая строка в этой таблице соответствует одному шифру замены вроде шифра Юлия Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифровку получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Этот очень распространенный вид шифра сохранился до наших дней. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

|  |  |
| --- | --- |
| сообщение: | ПРИЕЗЖАЮ ШЕСТОГО |
| ключ: | АГАВААГАВААГАВАА |
| шифровка: | ПНИГЗЖЮЮЮАЕОТМГО |

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять почаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ.

## Практическая часть

Внешний вид текстового редактора "Блокнот" с функцией шифрования-дешифрования классическими криптографическими методами представлен на рисунке 1.

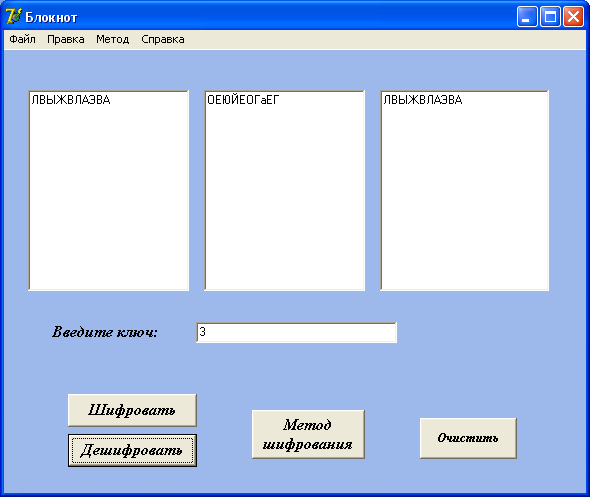


Рисунок 1 - Главная форма текстового редактора

В текстовом редакторе имеются меню "Файл" (рисунок 2), "Правка" (рисунок 3), "Метод" (рисунок 4), "Справка" (рисунок 5).

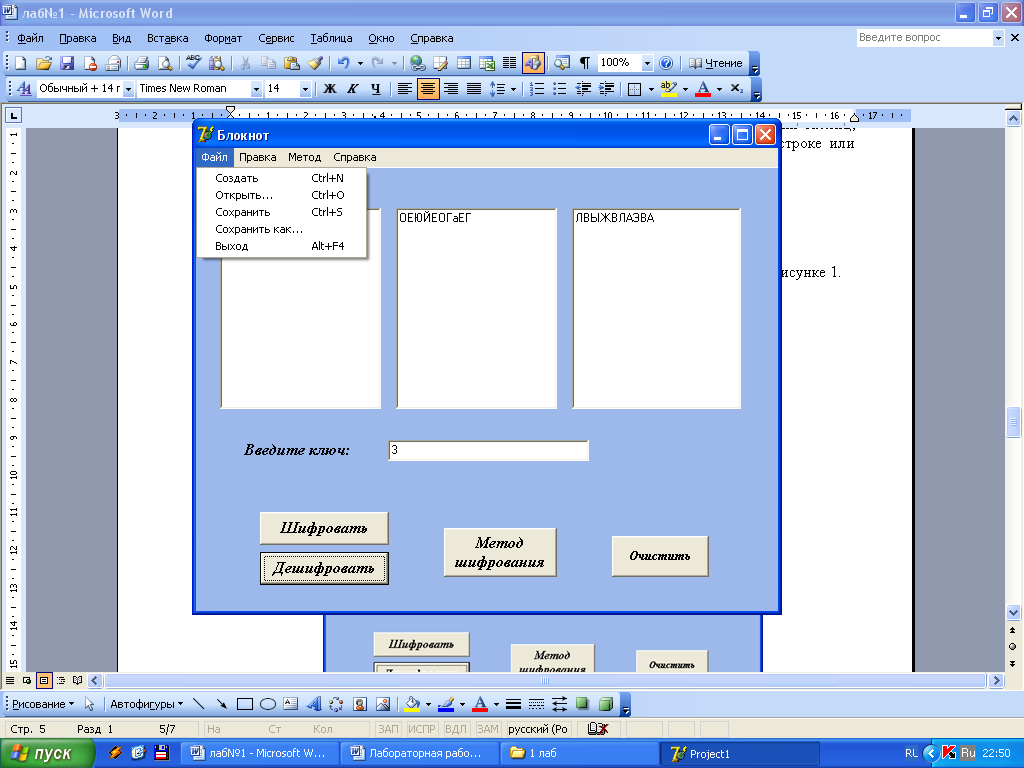


Рисунок 2 - Меню "Файл" текстового редактора.

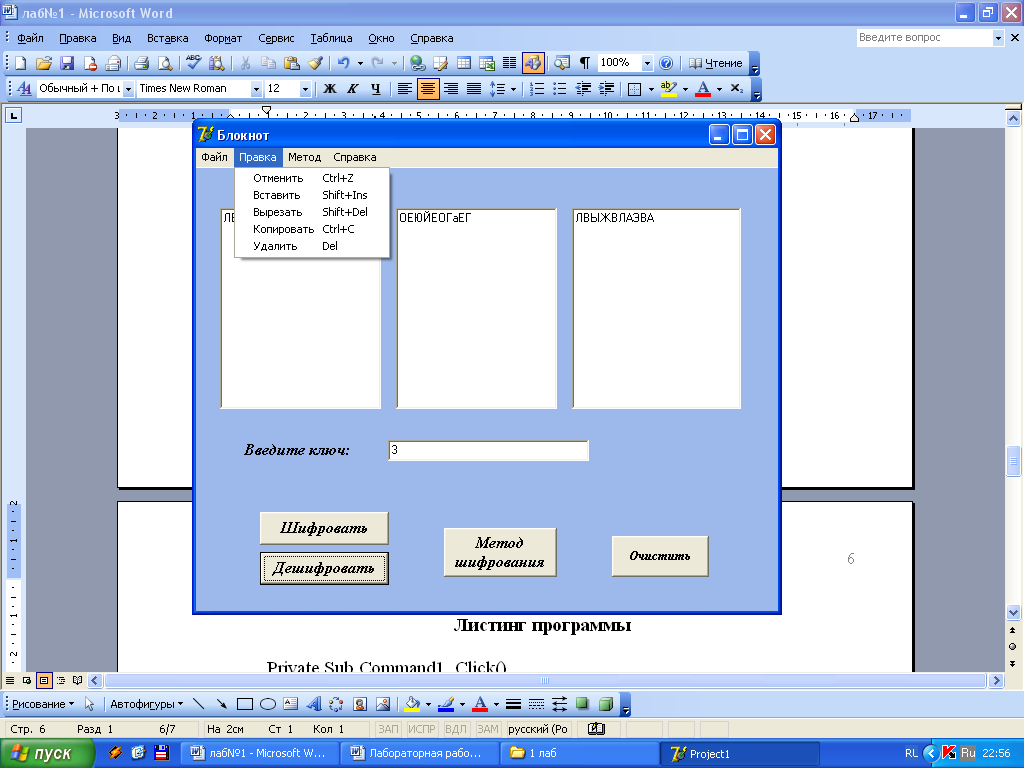


Рисунок 3 - Меню "Правка" текстового редактора

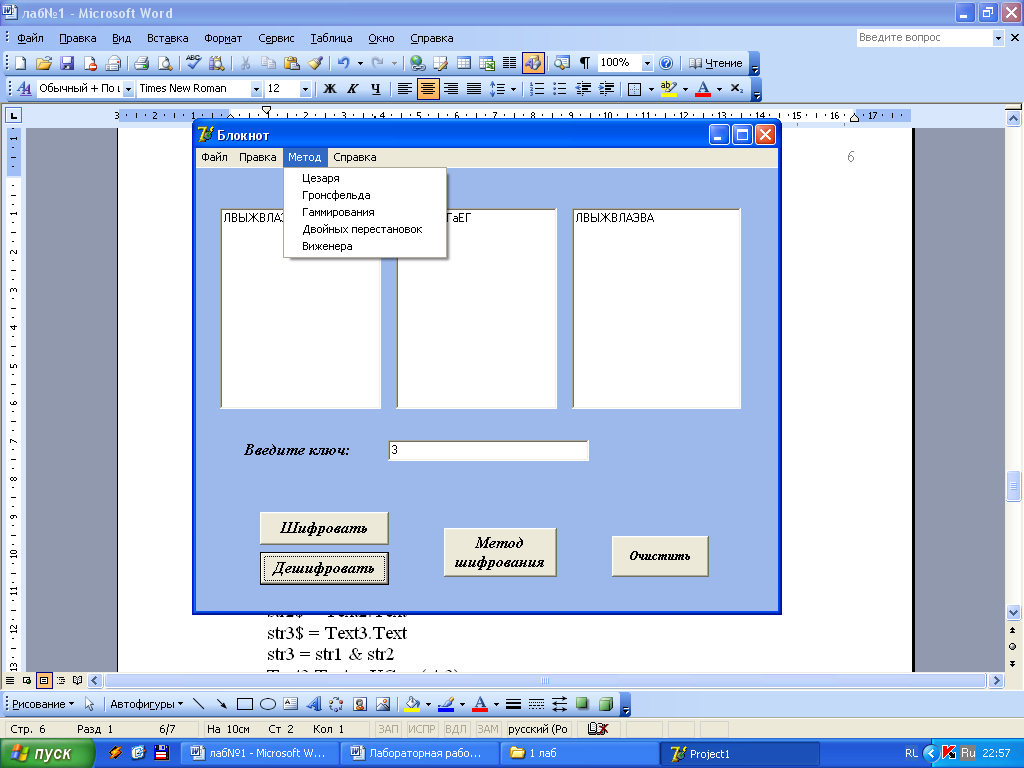


Рисунок 4 - Меню "Метод" текстового редактора

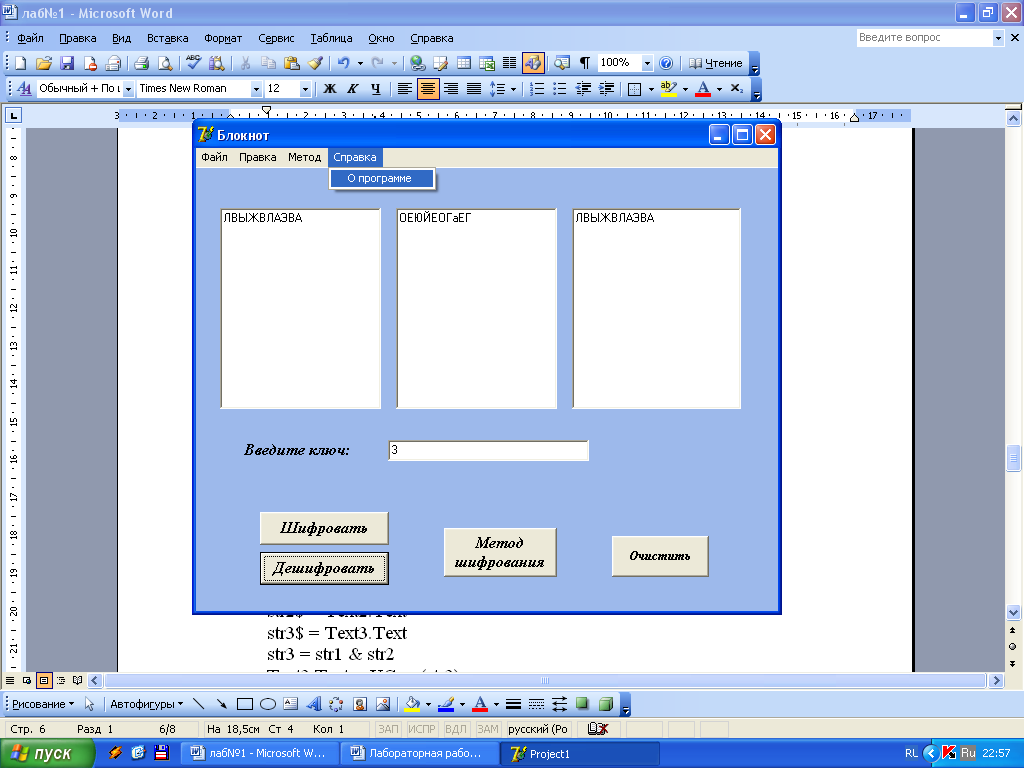


Рисунок 5 - Меню "Справка" текстового редактора

Пользователь также может выбрать метод шифрования при нажатии кнопки "Метод шифрования", при этом появится окно "Метод шифрования", показанный на рисунке 6.

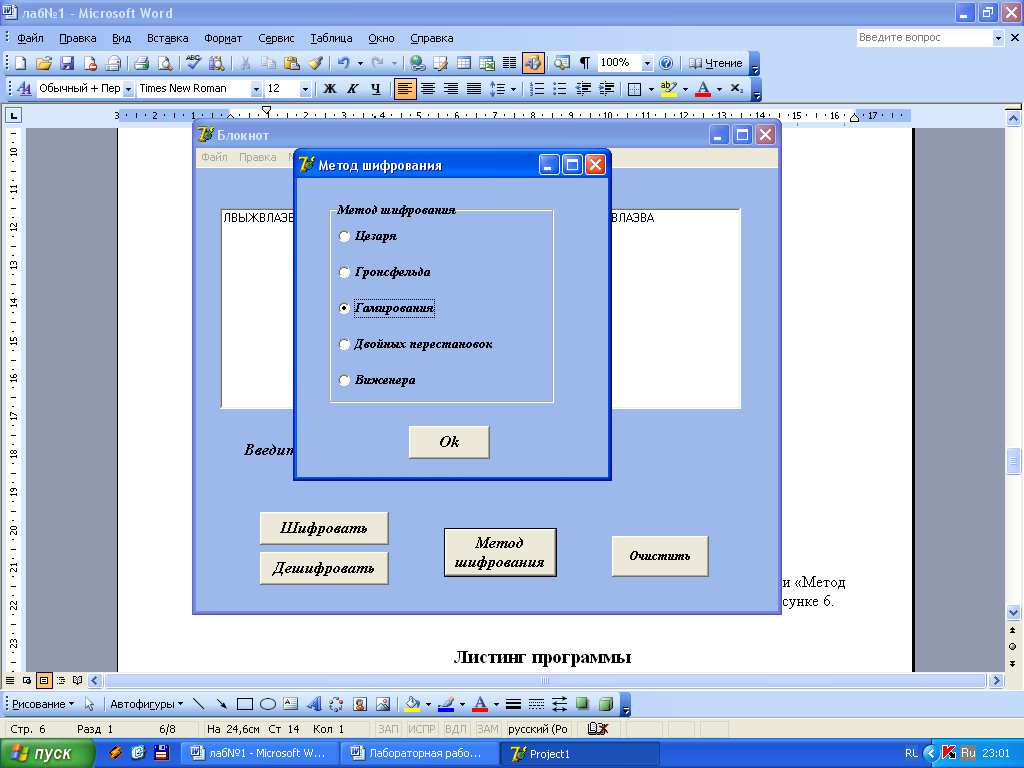


Рисунок 6 - Окно "Метод шифрования" текстового редактора

## Вывод

В результате выполнения данной курсовой работы, я ознакомилась с классическими методами шифрования. А также изучила принцип программной реализации классических криптографических методов: метода Цезаря; метода Гронсфельда; метода гаммирования; метода двойных перестановок; метода замены с использованием таблицы Виженера. Я смогла, применяя свои знания в области программирования, реализовать их программно.

## Листинг программы

procedure TForm1. N23Click (Sender: TObject);

begin

form2. SHOWMODAL;

end;

procedure TForm1. N24Click (Sender: TObject);

begin

Form3. SHOWMODAL;

end;

procedure TForm1. N5Click (Sender: TObject);

var i: integer;

begin

for i: =0 to m2. Lines. Count-1 do

m2. Lines [i]: ='';

for i: =0 to m1. Lines. Count-1 do

m1. Lines [i]: =''; // очистка memo1

m1. SetFocus;

end;

procedure TForm1. N6Click (Sender: TObject);

var

i: integer;

begin

OpenDialog1. Filter: = 'Текстовые файлы| \*. txt';

if OpenDialog1. Execute then

begin

EdFile: =OpenDialog1. FileName; {в переменную присваиваем

имя и полный путь к файлу}

m1. Lines. LoadFromFile (EdFile);

end;

end;

procedure TForm1. N7Click (Sender: TObject);

begin

saveDialog1. Filter: = 'Текстовые файлы| \*. txt';

if saveDialog1. Execute then

begin

EdFile: =SaveDialog1. FileName; // сохранение файла

m2. Lines. SaveToFile (EdFile);

end;

end;

procedure TForm1. N8Click (Sender: TObject);

begin

if saveDialog1. Execute then

begin

EdFile: =SaveDialog1. FileName; // сохранение файла

m2. Lines. SaveToFile (EdFile);

end;

end;

procedure TForm1. N10Click (Sender: TObject);

begin

Form1. Close;

end;

procedure TForm1. N12Click (Sender: TObject);

begin

m1. PasteFromClipboard; // вставка

end;

procedure TForm1. N14Click (Sender: TObject);

begin

m1. CopyToClipboard; // копирование

m2. CopyToClipboard;

end;

procedure TForm1. N13Click (Sender: TObject);

begin

m1. CutToClipboard; // Вырезание

end;

procedure TForm1. N15Click (Sender: TObject);

begin

m1. SelText: =''; // Удаление

m2. SelText: ='';

m3. SelText: ='';

end;

procedure TForm1. N18Click (Sender: TObject);

var i: integer;

begin

for i: =0 to m2. Lines. Count-1 do

m2. Lines [i]: ='';

m1. SetFocus;

MessageDlg ('Выберите метод щифрования! ', mtConfirmation, [mbOk], 0);

end;

procedure TForm1. Button1Click (Sender: TObject);

begin

form4. Showmodal;

end;

procedure TForm1. B1Click (Sender: TObject);

label 1,2,3,4,5,6,7;

var

SL: TStringList;

Al,a3,A,st,R,b,c,c2: string; D, MyChr: char;

dl, i,j,m,g,n,l,h,Summa,NewCode,k,p,x: integer;

A1: ARRAY [1. .34,1. .34] of integer;

a2: array [1. .8] of integer;

mas: array [1. .11,1. .11] of char;

mas1: array [1. .11] of char;

t: STRing [8] ; c1: STRing [8] ;

begin

if form4. radiogroup1. ItemIndex=-1 then

MessageDlg ('Выберите метод щифрования! ', mtConfirmation, [mbOk], 0);

if form4. RadioGroup1. ItemIndex=0 then

begin

M2. Clear; m3. Clear;

Al: ='';

m: =StrToInt (Edit1. Text);

SL: = TStringList. Create;

SL. Clear;

for i: = 0 to m1. Lines. Count-1 do

begin

A: = m1. Lines [i] ;

For j: =32 to 255 do

Al: =Al + Chr (j);

R: ='';

for j: = 1 to Length (A) do

begin

MyChr: =A [j] ;

n: =Pos (MyChr, Al);

If n = 0

Then R: =R + MyChr

Else

Begin

Summa: =n + m;

If Summa < 225 // Если предполагаемый номер символа попадает в алфавит

Then NewCode: =Summa

Else NewCode: = 32 - 1 + (Summa - 255);

R: =R+ Al [NewCode] ;

End;

end;

SL. Add (R);

end;

m2. Clear;

m2. Lines: = SL;

SL. Free;

end;

if form4. RadioGroup1. ItemIndex=1 then

begin

M2. Clear; m3. Clear;

c: =''; a: =''; b: ='';

A: = m1. Text;

b: =edit1. Text;

1: n: =length (b);

dl: =length (a);

if n>dl then

delete (b,dl+1,n) else

begin

c: =copy (b,1,n);

insert (c,b,n+1); goto 1;

end;

for i: =1 to dl do

begin

p: =ord (a [i]) +strtoint (b [i]);

m2. Text: =m2. text+chr (p);

end;

end;

if form4. RadioGroup1. ItemIndex=2 then

begin

M2. Clear; m3. Clear;

st: =''; c: =''; a: =''; b: ='';

A: = m1. Text;

randomize;

for i: =1 to 4 do

st: =st+chr (i+random (215) +40);

edit1. Text: =st;

4: n: =length (st);

dl: =length (a);

if n>dl then

delete (st,dl+1,n) else

begin

c: =copy (st,1,n);

insert (c,st,n+1); goto 4;

end;

for i: =1 to dl do

begin

k: =ord (a [i]) xor ord (st [i]);

m2. Text: =m2. text+chr (k);

end;

end;

if form4. RadioGroup1. ItemIndex=3 then

BEGIN

M2. Clear; m3. Clear;

A: =''; B: =''; c: ='';

A: =EDIT1. Text;

b: =edit2. Text;

c: =m1. Text;

n: = length (a);

k: = length (b);

if n<>k then

begin

MessageDlg ('Число цифр в ключах должны совпадать! ', mtConfirmation, [mbOk], 0);

edit1. Clear; edit2. Clear; GOTO 7;

end;

5: for j: =2 to k+1 do

mas [1,j]: =a [j-1] ;

for j: =2 to n+1 do

mas [j,1]: =b [j-1] ;

for i: =2 to k+1 do

for j: =2 to n+1 do

begin

if c<>'' then

begin

mas [i,j]: =c [1] ;

delete (c,1,1) end

else

mas [i,j]: =' ';

end;

for i: =n+1 downto 2 do

for j: =n+1 downto 2 do

if ord (mas [1, i]) >ord (mas [1,j]) then

for h: =1 to n+1 do

begin

mas1 [h]: =mas [h, i] ;

mas [h, i]: =mas [h,j] ;

mas [h,j]: =mas1 [h] ;

end;

for i: =n+1 downto 2 do

for j: =n+1 downto 2 do

if ord (mas [i,1]) >ord (mas [j,1]) then

for h: =1 to n+1 do

begin

mas1 [h]: =mas [i,h] ;

mas [i,h]: =mas [j,h] ;

mas [j,h]: =mas1 [h] ;

end;

for i: =2 to n+1 do

for j: =2 to n+1 do

m2. Text: =m2. Text+mas [i,j] ;

if c<>'' then goto 5;

7: end;

if form4. RadioGroup1. ItemIndex=4 then

begin

M2. Clear; m3. Clear;

c: =''; a: =''; b: ='';

A: = M1. Text;

b: =edit1. Text;

for i: =0 to m1. Lines. Count-1 do

begin

a3: ='';

a3: =m1. Lines [i] ;

for j: =1 to length (a3) do

begin

if ord (a3 [j]) = 184 then

begin

MessageDlg ('Можно вводить только прописные буквы! ', mtConfirmation, [mbOk], 0);

m1. Clear;

M2. Clear;

GOTO 6;

end;

if (ord (a3 [j]) >= 224) and (ord (a3 [j]) <= 255) then

begin

MessageDlg ('Можно вводить только прописные буквы! ', mtConfirmation, [mbOk], 0);

m1. Clear;

M2. Clear;

M3. Clear;

GOTO 6;

end;

end;

end;

2: n: =length (b);

dl: =length (a);

if length (b) >dl then

delete (b,length (a) +1,length (b)) else

begin

c: =copy (b,1,n);

insert (c,b,n+1); goto 2;

end;

for I: =1 to 34 do

for j: =1 to 34 do

begin

k: = j-i+1;

if k=0 then a1 [i,j]: =34 else

if k>0 then a1 [i,j]: =k else

a1 [i,j]: =34+k;

end;

for i: =1 to length (a) do

begin

if a [i] <>'' then

begin

if a [i] =' ' then l: =34 ELSE

if a [i] ='Ё' THEN l: =7 ELSE

BEGIN

n: =ord (a [i]) - 191;

if (n>=1) and (n<7) then l: =n else

if (n>=7) and (n<34) then l: =n+1;

END;

end;

if b [i] <>'' then

begin

if b [i] =' ' then M: =34 ELSE

if b [i] ='Ё' THEN m: =7 ELSE

BEGIN

n: =ord (b [i]) - 191;

if (n>=1) and (n<7) then m: =n else

if (n>=7) and (n<34) then m: =n+1;

END;

end;

g: =a1 [M,L] ;

if g=7 then d: ='Ё' else

if g=34 then d: =' ' else

begin

if (g>=1) and (g<7) then

d: =chr (g+191);

if (g>=8) and (g<34) then

d: =chr (g-1+191);

end;

m2. Text: =m2. Text+d;

end;

6: end;

end;

procedure TForm1. N19Click (Sender: TObject);

begin

form4. RadioGroup1. ItemIndex: =0;

b1. SetFocus; M2. Clear; M3. Clear;

edit2. Visible: =false;

label2. Visible: =false;

end;

procedure TForm1. FormActivate (Sender: TObject);

begin

m1. SetFocus;

end;

procedure TForm1. B2Click (Sender: TObject);

label 1,2,3,4,5,6,7;

var SL: TStringList;

Al,A,st,R,b,c,c2: string; D, MyChr: char;

dl, i,j,m,g,h,n,l,S,NewCode,k,p,x: integer;

A1: ARRAY [1. .34,1. .34] of integer;

a2: array [1. .8] of integer; t: STRing [8] ;

mas: array [1. .11,1. .11] of char;

mas2: array [1. .11,1. .11] of char;

mas1: array [1. .11] of char; c1: STRing [8] ;

begin

if form4. RadioGroup1. ItemIndex=0 then

begin

Al: ='';

m: =StrToInt (Edit1. Text);

SL: = TStringList. Create;

SL. Clear;

for i: = 0 to m2. Lines. Count-1 do

begin

A: = m2. Lines [i] ;

For j: =32 to 255 do

Al: =Al + Chr (j);

R: ='';

for j: = 1 to Length (A) do

begin

MyChr: =A [j] ;

n: =Pos (MyChr, Al);

If n = 0

Then R: =R + MyChr

Else

Begin

S: =n - m;

If S > 0 // Если предполагаемый номер символа попадает в алфавит

Then NewCode: =S

Else NewCode: = 224 + S;

R: =R+ Al [NewCode] ;

End;

end;

SL. Add (R);

end;

m3. Clear;

m3. Lines: = SL;

SL. Free;

end;

if form4. RadioGroup1. ItemIndex=1 then

begin

M3. Clear;

c: =''; a: =''; b: ='';

A: = m2. Text;

b: =edit1. Text;

1: n: =length (b);

dl: =length (a);

if n>dl then

delete (b,dl+1,n) else

begin

c: =copy (b,1,n);

insert (c,b,n+1); goto 1;

end;

for i: =1 to dl do

begin

p: =ord (a [i]) - strtoint (b [i]);

m3. Text: =m3. text+chr (p);

end;

end;

if form4. RadioGroup1. ItemIndex=2 then

begin

M3. Clear;

st: =''; c: =''; a: =''; b: ='';

A: = m2. Text;

st: =edit1. Text;

4: n: =length (st);

dl: =length (a);

if n>dl then

delete (st,dl+1,n) else

begin

c: =copy (st,1,n);

insert (c,st,n+1); goto 4;

end;

for i: =1 to dl do

begin

k: =ord (a [i]) xor ord (st [i]);

m3. Text: =m3. text+chr (k);

end;

end;

if form4. RadioGroup1. ItemIndex=3 then

BEGIN

M3. Clear;

A: =''; B: =''; c: ='';

A: =EDIT1. Text;

b: =edit2. Text;

c: =m2. Text;

n: = length (a);

k: = length (b);

if n<>k then

begin

MessageDlg ('Число цифр в ключах должны совпадать! ', mtConfirmation, [mbOk], 0);

edit1. Clear; edit2. Clear;

end;

5: for j: =2 to k+1 do

mas [1,j]: =a [j-1] ;

for j: =2 to n+1 do

mas [j,1]: =b [j-1] ;

for i: =n+1 downto 2 do

for j: =n+1 downto 2 do

if ord (mas [1, i]) >ord (mas [1,j]) then

begin

d: =mas [1, i] ;

mas [1, i]: =mas [1,j] ;

mas [1,j]: =d;

end;

for i: =n+1 downto 2 do

for j: =n+1 downto 2 do

if ord (mas [i,1]) >ord (mas [j,1]) then

begin

d: =mas [i,1] ;

mas [i,1]: =mas [j,1] ;

mas [j,1]: =d;

end;

for i: =2 to k+1 do

for j: =2 to n+1 do

begin

if c<>'' then

begin

mas [i,j]: =c [1] ;

delete (c,1,1) end

else

mas [i,j]: =' ';

end;

m3. Text: =m1. Text;

{for i: =2 to n+1 do

begin

g: =pos (mas [i,1],b); edit3. Text: =edit3. Text+inttostr (g);

for h: =1 to n+1 do

begin

mas1 [h]: =mas [i,h] ;

mas2 [g,h]: =mas1 [h] ;

end;

end;

for j: =2 to n+1 do

begin

g: =pos (mas [1,j],a);

for h: =1 to n+1 do

begin

mas1 [h]: =mas2 [h,j] ;

mas [h,g]: =mas1 [h] ;

end;

end;

for i: =2 to n+1 do

for j: =2 to n+1 do

m3. Text: =m3. Text+mas [i,j] ;

if c<>'' then goto 5; }

end;

if form4. RadioGroup1. ItemIndex=4 then

begin

M3. Clear;

c: =''; a: =''; b: ='';

A: = M2. Text;

b: =edit1. Text;

2: n: =length (b);

dl: =length (a);

if length (b) >dl then

delete (b,length (a) +1,length (b)) else

begin

c: =copy (b,1,n);

insert (c,b,n+1); goto 2;

end;

for I: =1 to 34 do

for j: =1 to 34 do

begin

k: = j-i+1;

if k=0 then a1 [i,j]: =34 else

if k>0 then a1 [i,j]: =k else

a1 [i,j]: =34+k;

end;

for i: =1 to length (A) do

BEGIN

if b [i] <>'' then

begin

if b [i] =' ' then M: =34 ELSE

if b [i] ='Ё' THEN m: =7 ELSE

BEGIN

n: =ord (b [i]) - 191;

if (n>=1) and (n<7) then m: =n else

if (n>=7) and (n<34) then m: =n+1;

END;

end;

if a [i] ='Ё' then g: =7 else

if a [i] =' ' then g: =34 else

begin

x: =ord (a [i]) - 191;

if (x>=1) and (x<7) then

g: =x else

if (X>=7) and (X<34) then g: =x+1;

end;

for j: =1 to 34 do

if a1 [m,j] =g then

BEGIN

l: =j;

if l=7 then d: ='Ё' else

if l=34 then d: =' ' else

begin

if (l>=1) and (l<7) then

d: =chr (l+191);

if (l>=8) and (l<34) then

d: =chr (l-1+191);

END;

end;

m3. Text: =m3. Text+d;

end;

end;

end;

procedure TForm1. N20Click (Sender: TObject);

begin

form4. RadioGroup1. ItemIndex: =1;

b1. SetFocus; M2. Clear; M3. Clear;

edit2. Visible: =false;

label2. Visible: =false;

end;

procedure TForm1. Button2Click (Sender: TObject);

begin

m1. Clear;

m2. Clear;

m3. Clear;

edit1. Clear;

edit2. Clear;

end;

procedure TForm1. N21Click (Sender: TObject);

begin

form4. RadioGroup1. ItemIndex: =2;

b1. SetFocus; M2. Clear; M3. Clear; edit2. Visible: =false;

label2. Visible: =false;

end;

procedure TForm1. N22Click (Sender: TObject);

begin

M2. Clear; M3. Clear;

form4. RadioGroup1. ItemIndex: =3;

if form4. radiogroup1. ItemIndex=3 then

begin

edit2. Visible: =true;

label2. Visible: =true;

end

else

begin

edit2. Visible: =false;

label2. Visible: =false;

end;

b1. SetFocus; m3. Clear;

end;

procedure TForm1. N9Click (Sender: TObject);

begin

form4. RadioGroup1. ItemIndex: =4; edit2. Visible: =false;

label2. Visible: =false;

b1. SetFocus; M2. Clear; M3. Clear;

end;

procedure TForm1. N11Click (Sender: TObject);

begin

m2. Undo;

end;

end.

**unit Unit4;**

interface

uses

Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,

Dialogs, StdCtrls, ExtCtrls;

type

TForm4 = class (TForm)

RadioGroup1: TRadioGroup;

Button1: TButton;

procedure Button1Click (Sender: TObject);

procedure FormActivate (Sender: TObject);

private

{ Private declarations }

public

{ Public declarations }

end;

var

Form4: TForm4;

implementation

uses Unit1;

{$R \*. dfm}

procedure TForm4. Button1Click (Sender: TObject);

begin

if radiogroup1. ItemIndex=-1 then

MessageDlg ('Выберите метод щифрования! ', mtConfirmation, [mbOk], 0)

else

begin

form1. Show;

if radiogroup1. ItemIndex=3 then

begin

FORM1. M2. Clear; form1. M3. Clear;

form1. edit2. Visible: =true;

form1. label2. Visible: =true;

end

else

begin

form1. edit2. Visible: =false;

form1. label2. Visible: =false;

end;

if radiogroup1. ItemIndex=0 then

begin

form1. M2. Clear; form1. M3. Clear; end;

if radiogroup1. ItemIndex=1 then

begin

form1. M2. Clear; form1. M3. Clear; end;

if radiogroup1. ItemIndex=2 then

begin

form1. M2. Clear; form1. M3. Clear; end;

if radiogroup1. ItemIndex=4 then

begin

form1. M2. Clear; form1. M3. Clear; end;

form4. Close;

end;

end;

procedure TForm4. FormActivate (Sender: TObject);

begin

Radiogroup1. ItemIndex: =-1;

end;

end.