**Шифрование в Delphi**

Данные надо беречь. Сам посуди, обидно, если открытие ценой в сто миллионов енотов или рецепт безалкогольной водки, над которым ты корпел три вечера в мрачном подвале нелегального компьютерного клуба, — уплывет к злостному ленивому конкуренту, который, пользуясь твоим похмельем, наложил грязную лапу на приватные дискеты с ценнейшей инфой?! Дальше можно не продолжать. Шифруем, шифруем, шифруем!..

Добрый дядюшка Borland предоставил нам несколько занятных функций для работы со строками, о которых не все знают. Сосредоточены они в модуле StrUtils.pas. Такие функции, как RightStr, LeftStr совмещают стандартные команды Copy и Delete: так, LeftStr возвращает значение левой части строки до указанной вами позиции (что вытворяет RightStr, догадайся сам), а функция ReverseString и вовсе делает зеркальное отображение данной строки: 321 вместо 123. Используем ее в особенности, чтобы осложнить жизнь хитрому дешифровщику.

Алгоритм шифрования будет прост, как Win 3.1. С каждым символом кодируемого документа проделаем следующее:

1. Преобразуем символ в число командой Ord.

2. Преобразуем каждый символ пользовательского пароля в число и сумму этих чисел прибавим к полученному в пункте 1.

3. От результата отнимаем число, равное позиции данного символа. То есть буковки будут шифроваться по-разному в зависимости от их позиции в строке :).

4. То, что получилось, запишем обратно из чисел в символы командой Chr. Как видишь, после всех наших манипуляций этот символ уже будет другим.

5. Запишем всю строку навыворот командой ReverseString.

Дешифровка, как ты догадываешься, будет производиться в обратном порядке.

Теперь, когда алгоритм намертво засел в голове, реализуем соответствующую программу. Внимание! Не исключено, что это будет первая твоя программа с настоящим синтаксисом команд:

<команда> <путь> <пароль>

— так будет выглядеть он в консоли нашего приложения (да, оно будет консольным!). Команд всего две: crypt и decrypt — соответственно зашифровать и дешифровать файл, путь к которому указывается после пробела, а затем — твой пароль. НЕ ЗАБУДЬ ЕГО! Предупреждаю совершенно серьезно. Запомнил? В бой!

Crypt C:\file.txt linuxmustsurvive

— закодируем File.txt. Результат (зашифрованный текст) сохраниться в той же директории, что и исполняемый файл нашего приложения под именем Translated\_File.txt.

Decrypt C:\Translated\_file.txt linuxmustsurvive

— дешифровка.

Реализовывается это вот как:

program Crypter;

{$APPTYPE CONSOLE}

uses

SysUtils,

StrUtils; //!!

var

F, //входящий файл

F1: TextFile; //результат (файл с переводом)

ToDo, FileName, PassW, Line, TranslatedFile: string;

position, IsCrypt: integer;

//находим сумму числовых значений символов пароля

function Password(Psw: string): integer;

var

i,res: integer;

begin

res:=0;

for i:=1 to Length(psw) do res:=res+ord(psw[i]);

result:=res;

end;

function Crypt(CryptStr: string): string;

var

s: string;

i: integer;

begin

if CryptStr<>EmptyStr then

for i:=1 to Length(CryptStr) do begin

s:=LeftStr(CryptStr,1);

CryptStr:=RightStr(CryptStr,Length CryptStr)-1);

//ШИФРОВКА:

s:=chr(ord(s[1])+Password(PassW)-i);

result:=result+s;

end;

result:=ReverseString(result);

end;

function Decrypt(DecryptStr: String): String;

var

i: integer;

s: String;

begin

DecryptStr:=ReverseString(DecryptStr);

if DecryptStr<>EmptyStr then

for i:=1 to Length(DeCryptStr) do begin

s:=LeftStr(DeCryptStr,1);

DeCryptStr:=RightStr(DeCryptStr,Length DeCryptStr)-1);

//ДЕШИФРОВКА:

result:=result+chr(ord(s[1])-password(PassW)+i);

end;

end;

begin

while true do begin

isCrypt:=0;

writeln(#10+'Crypter >'+#10);

//Какую команду ввел юзер?

readln(ToDo);

if UpperCase(ToDo)='EXIT' then Exit;

if AnsiContainsText(ToDo,'decrypt') then isCrypt:=1

else if AnsiContainsText(ToDo,'crypt') then isCrypt:=2;

//прочитав команду, удаляем ее из строки и читаем дальше

position:=pos(' ',ToDo);

if position>0 then ToDo:=RightStr(ToDo,Length(ToDo)-position);

//Читаем путь к файлу

position:=pos(' ',ToDo);

if position>0 then FileName:=LeftStr(ToDo,position-1);

//Читаем пароль

PassW:=RightStr(ToDo,Length(ToDo)-position);

//Всё правильно? Начинаем!

if (isCrypt<=0) or (PassW=EmptyStr) or (not FileExists(FileName)) then writeln('Wrong command')

else begin

TranslatedFile:=ExtractFilePath(paramStr(0)) + 'translated\_' + ExtractFileName(FileName);

//соединяемся с файлами

AssignFile(F, FileName);

AssignFile(F1, TranslatedFile);

//переходим в начало файла

Rewrite(F1);

Reset(F);

//читаем строки, пока не дойдем до конца файла

while not EOF(F) do begin

//читаем из переводимого файла

ReadLn(F, Line);

if isCrypt=1 then Line:=Decrypt(Line);

if isCrypt=2 then Line:=Crypt(Line);

//записываем в файл с переводом

Writeln(F1, Line);

end;

//отсоединямся от файлов

CloseFile(F);

CloseFile(F1);

end;

end;

end.

Вот, собственно, и всё. Еще раз напоминаю, что результат (файл с переводом) сохранится В ТОЙ ЖЕ ДИРЕКТОРИИ, что и наше приложение, а не в той, где лежит исходный файл. В заключение процитирую отрывок из статьи «Криптография в C++» в номере 3.03 журнала «Хакер»:

(с) Николай «GorluM» Андреев

Но я хочу тебя предупредить: в нашей стране, согласно указу № 334 от 1995 года, производить и распространять любые шифрующие средства можно, только имея лицензию ФАПСИ. Соответственно, шифровать нельзя :). Поэтому пиши программы только для личного пользования и только в познавательных целях.