```
{****************************************************************
 *
 * Project  : CryptoBox AES Crypto Series
 * App Name : 258_AES_cryptobox2.txt, loc's = 388
 * Purpose  : crypt & decrypt a file with AES symmetric keys
            : example for tutorial 13
 * History  : system for mX3.2, internal random generator, newdir
            : 220_CipherBox_form2.txt, loc's = 312
            : LockBox3 implemented for more acurate Standard
            : SHA256 integration
 * ToDo     : check if key or pasword is loaded!, rename encrypted file to orig
            : code a better password dialog to reset the password
 ****************************************************************}

Program CipherBox3_FORM_Lab;

const LEFTBASE = 20;
      TOPBASE = 25;
      MEDIAPATH =  'exercices\';
      KEYPATH = 'crypt\';
      CIPHERLOG = 'cipherbox_log2.txt';

var
  mpan: TPanel;
  mPlayer: TMediaPlayer;   //for future use
  inFrm: TForm;
  cLstbox: TListbox;
  stat: TStatusbar;
  idx: integer;
  selectFile, cryptlog, AESpassw: string;


function MSecToTime(mSec: Int64): string;
var dt: TDateTime;
begin
  dt:= (mSec/1000/86400);  //SecsPerDay;
  Result:= FormatDateTime('" song length is:" nn:ss:zzz',dt);
end;

procedure OpenCD(self: TObject);
begin
  OpenCDDrive;
end;


//******************************Event Handler**********************************
procedure CloseCryptClick(Sender: TObject; var action: TCloseAction);
begin
  //Form1.Close;  free 308 kByte
  if MessageDlg('Wanna Leave Crypt?',mtConfirmation,[mbYes, mbNo],0) = mrYes then begin
    //inFrm.Free;
    MPlayer.Close;
    MPlayer.Free;
    action:= caFree;
 end else
    Action:= caNone;
end;

procedure CryptoButtonCloseClick(sender: TObject);
begin
  //mbitmap.Free;
  inFrm.Close;
end;

//AES CryptoBox
procedure BtnGetPassword(Sender: TObject);
begin
  AESpassw:= InputBox('AES CryptoBox Password' ,'Enter Password:','password');
  clstBox.Items.Add('Password is set! at: '+DateTimeToStr(Now));
  {with TPasswordDlg.Create(NIL) do begin
    showmodal;
    if modalresult = mrOK then begin
    AESpassw:= password.Text;
        with clstBox.Items do begin
         Add('Password is set! at: '+DateTimeToStr(Now));
       end;
    end else begin
    //if cancelbtn.modalresult = mrCancel then begin
     password.Text:= '';
     AESpassw:= '';
     clstBox.Items.Add('Password empty reset at: '+DateTimeToStr(Now));
     //showmessage(AESpassw);  debig
    end;
    Free;}
  end;

```

```

procedure EncryptMediaAES(sender: TObject);
begin
  if AESpassw <> '' then begin
    if PromptForFileName(selectFile,'Files(*.*)|*.*',//others
                      '', 'Select your file to crypt', MEDIAPATH, False)
    then begin
     //Display this full file/path value
      mpan.font.color:= clyellow;
      mpan.font.size:= 18;
      mpan.caption:= ExtractFileName(selectFile)+' encrypt...';
      Application.ProcessMessages;
      Screen.Cursor:= crHourglass;
      with clstBox.Items do begin
        Add('SHA256 Hash of: '+ExtractFileName(selectFile));
        Add('is: '+ComputeSHA256(selectFile,'F'));
        idx:= Add('File to Crypt: '+ExtractFileName(selectFile));
        stat.SimpleText:= clstBox.items[idx];
      end;
      with TStopwatch.Create do begin
        Start;
        AESSymetricExecute(selectFile, selectFile+'_encrypt',AESpassw);
        mpan.font.color:= clblue;
        mpan.font.size:= 30;
        mpan.caption:= 'File Encrypted!';
        Screen.Cursor:= crDefault;
        Stop;
        clstBox.Items.Add('Time consuming: ' +GetValueStr +' of: '+
              inttoStr(getFileSize(selectFile))+' File Size');
        Free;
      end;
      cLstbox.Items.Add('Crypted file: '+ExtractFileName(selectFile)+'_encrypt');
      WriteLog(cryptLog, clstbox.items.text)
    end;
  end else Showmessage('Set your password first!');
end;


procedure DecryptMediaAES(sender: TObject);
var clearout: string;
begin
  if AESpassw <> '' then begin
    if PromptForFileName(selectFile,'Files(*_encrypt)|*_encrypt',//others
                      '', 'Select your file to decrypt', MEDIAPATH, False)
    then begin
      // Display this full file/path value
      mpan.font.color:= clyellow;
      mpan.font.size:= 18;
      mpan.caption:= ExtractFileName(selectFile)+' decrypt...';
      idx:= cLstbox.Items.Add('File to Decrypt: '+ExtractFileName(selectFile));
      stat.SimpleText:= cLstbox.Items[idx];
      Application.ProcessMessages;
      Screen.Cursor:= crHourglass;
      with TStopwatch.Create do begin
        Start;
        AESDecryptFile(selectFile+'_decrypt',selectFile,AESpassw);
        clearout:= selectFile+'_decrypt';
        Delete(clearout, length(clearout)-15, 8); //-7!
        RenameFile(selectFile+'_decrypt', clearout);
        Screen.Cursor:= crDefault;
        Stop;
        clstBox.Items.Add('Time consuming: ' +GetValueStr +' of: '+
              intToStr(getFileSize(clearout))+' File Size');
        Free;
      end;
      mpan.font.color:= clGreen;  //clLime
      mpan.font.size:= 30;
      mpan.caption:= 'File Decrypted!';
      with clstBox.Items do begin
        Add('SHA256 Hash of '+ExtractFileName(clearout));
        Add('is: '+ComputeSHA256(clearout,'F'));
        Add('File Decrypted as: '+ExtractFileName(clearout));
      end;
      WriteLog(cryptLog, clstbox.items.text)
    end;
  end else Showmessage('Set your password first!');
end;

//*************************************Form Creator*************************
procedure SetCryptFormAES;
var
  mi, mi1, mi2: TMenuItem;
  mt: TMainMenu;
  mlbl, mlbl1: TLabel;
begin
  inFrm:= TForm.Create(self);
```

```
mLbl:= TLabel.create(inFrm);
mLbl1:= TLabel.create(inFrm);
mpan:= TPanel.Create(inFrm);
stat:= TStatusbar.Create(inFrm);
cLstbox:= TListbox.create(inFrm);

with inFrm do begin
   caption:= '********CryptoBox3 AES256 and SHA256************';
   height:= 610;
   width:= 1180;
   //color:= clred;
   Position:= poScreenCenter;
   onClose:= @CloseCryptClick;
   Show;
 end;
 with mpan do begin
   caption:= '****CryptoBox_AES256_SHA256****';
   parent:= inFrm;
   SetBounds(LEFTBASE+10,TOPBASE+40,416,400);
   color:= clsilver;
   font.color:= clyellow;
   font.size:= 20;
   Show;
 end;
with cLstbox do begin
  parent:= inFrm;
  SetBounds(LEFTBASE+450, TOPBASE+40, 670, 400);
  font.size:= 10;
  color:= clYellow;
  //onClick:= ChangeKey;
end;
with TBitBtn.Create(inFrm) do begin
  Parent:= inFrm;
  setBounds(LEFTBASE+490,TOPBASE+460,150,40);
  caption:= '&Close';
  font.size:= 12;
  glyph.LoadFromResourceName(HINSTANCE,'CL_MPSTOP');
  onclick:= @CryptoButtonCloseClick; //CloseCryptClick;
end;
with TBitBtn.Create(inFrm) do begin
  Parent:= inFrm;
  setbounds(LEFTBASE+ 650, TOPBASE+ 460,150, 40);
  caption:= 'File to &Encrypt';
  font.size:= 12;
  //font.Style:= [fsBold];
  glyph.LoadFromResourceName(getHINSTANCE,'CL_MPNEXT');
  onclick:= @EncryptMediaAES;
end;
with TBitBtn.Create(inFrm) do begin
  Parent:= inFrm;
  setbounds(LEFTBASE+ 810, TOPBASE+460,150, 40);
  caption:= 'File to &Decrypt';
  font.size:= 12;
  glyph.LoadFromResourceName(getHINSTANCE,'CL_MPPLAY');
  onclick:= @DecryptMediaAES;
end;
with TBitBtn.Create(inFrm) do begin
  Parent:= inFrm;
  setbounds(LEFTBASE+ 970, TOPBASE+460,150, 40);
  caption:= 'Enter &Password!';
  font.size:= 12;
  glyph.LoadFromResourceName(getHINSTANCE,'CL_MPPAUSE');
  //event handler
  onclick:= @BtngetPassword;
end;
with mlbl do begin
  parent:= inFrm;
  setbounds(LEFTBASE+15,TOPBASE-15,180,20);
  font.size:= 32;
  font.color:= clred;
  font.style:= [fsunderline];
  caption:= 'AES CryptoBox';
end;
with mlbl1 do begin
  parent:= inFrm;
  setbounds(LEFTBASE+455,TOPBASE-1,180,20);
  font.size:= 20;
  font.color:= clred;
  caption:= 'Log Register:';
end;
mt:= TMainMenu.Create(infrm);
with mt do begin
 //parent:= frmMon;
end;
mi:= TMenuItem.Create(mt);
mi1:= TMenuItem.Create(mt);
```

```
  mi2:= TMenuItem.Create(mt);
  with mi do begin
    //parent:= frmMon;
    Caption:='Encrypt File';
    Name:='ITEM';
    mt.Items.Add(mi);
    OnClick:= @EncryptMediaAES;
  end;
  with mi1 do begin
    Caption:='Decrypt File';
    Name:='ITEM2';
    mt.Items.Add(mi1) ;
    OnClick:= @DecryptMediaAES;
  end;
  with mi2 do begin
    Caption:='Set Password';
    Name:='ITEM3';
    mt.Items.Add(mi2);
    OnClick:= @BtngetPassword;
  end;
  with Stat do begin
    parent:= inFrm;
    stat.SimplePanel:= true;
  end;
  MPlayer:= TMediaPlayer.create(self);
  with MPlayer do begin
    parent:= inFrm;
    height:= 38;
    top:= TOPBASE + 460;
    left:= LEFTBASE+ 10;
    Display:= mpan;   //for video show
  end;
  if DirectoryExists(ExePath+KEYPATH) = false then
    CreateDir(ExePath + KEYPATH);
  cLstbox.Items.Add('Welcome to CryptoBox3 protecting your Data '+datetimetoStr(Now));
  idx:= cLstbox.Items.Add('Keypath is: '+ExePath+KEYPATH);
  stat.SimpleText:= cLstbox.Items[idx];
  cryptLog:= ExePath+CIPHERLOG;
  cLstbox.Items.Add('CryptoBox3 ready, Save or load a Password protected Cipher');
end;

//main app
begin
  SetCryptFormAES;
  if DirectoryExists(ExePath+KEYPATH) = false then
    CreateDir(ExePath+ KEYPATH);
   cryptLog:= ExePath+ CIPHERLOG;
   writeln('Machine: '+GetHostName)
   writeln('User: '+GetUserName)
   writeln('Instance: '+intToStr(getHinstance))
   writeln('Procid: '+intToStr(getProcessid))
   writeln('Processors: '+intToStr(GetNumberOfProcessors))
   WriteLog(cryptLog, memo2.text)
End.

//----------------------------------------------------------

cry-crypt-crypto-cryptologic
-----------------------------------------------------
Programmers never die, they just GOSUB without RETURN
```