File Encryption Using DES Algorithm

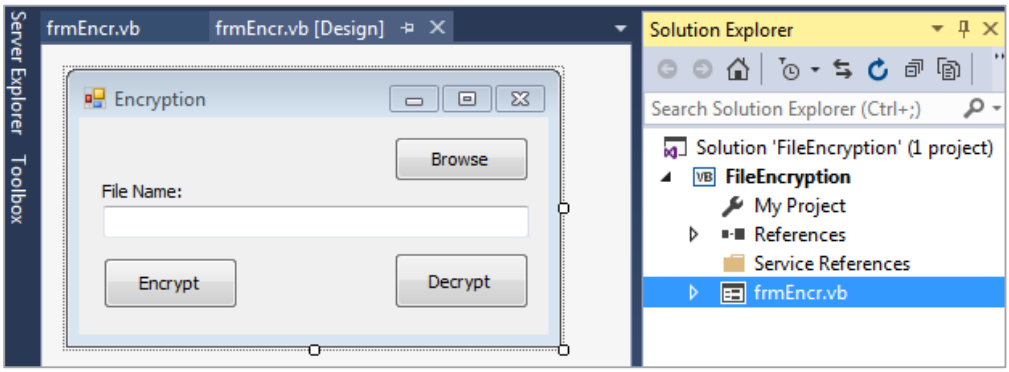
These guidelines show how implement file encryption/decryption using DES algorithm in VB.NET platform.
Time needed to accomplish this task: 20 - 30 minutes

GUI

- Create a new VB.NET project "Windows Form Application", change the project name and path according to your preferences.
- Create a new windows form (if it is not created by default), name it "frmEncr", and change its caption/text to "Encryption"
- In "frmEnc" form, create 1 textbox, 1 label, and 3 buttons and change their properties as follows:

Old Name	New Name	Caption/Text	Other Properties
TextBox1	txtInp		
Label1	lblInp	File Name:	
Button1	btnBrowse	Browse	
Button2	btnEnc	Encrypt	
Button3	btnDec	Decrypt	

- By the end of this step you should have something looks like the following picture:



Now… Let's do some coding…

Coding

- At the beginning, let's do some imports. Add these lines to the beginning of your "frmEncr.vb" file

```
Imports System
Imports System.IO
Imports System.Text
Imports System.Security.Cryptography
```

Note: The above imports help us to minimize the time needed to write the code.
With the above imports statements, instead of using statements like:

```
Dim DESx As New System.Security.Cryptography.DESCryptoServiceProvider
```

We will only need to write this instead:

```
Dim DESx As New DESCryptoServiceProvider
```

Both statements above will do the same, however the last one is shorter…

- At the beginning of "frmEncr" public class write the following:

```
Inherits System.Windows.Forms.Form
Private des As DESCryptoServiceProvider
```

Browsing for the file:

To select the file that you want to encrypt/decrypt, we will use "OpenFileDialog" tool that you can find it in the Toolbox under "Dialogs" subcategory.

- Drag and drop "OpenFileDialog" into your form. You will notice that this tool is added to under the divider below your form.
- Change the name of this tool from "OpenFileDialog1" to "OFD1"
- Double click on frmBrowse button. On btnBrowse_Click event, write the following code

```
OFD1.ShowDialog()
TxtInp.Text = OFD1.FileName
```

Note: The code above will show the OpenFileDialog "OFD1" to the user and let the user browse and select the file. When a file is selected, the filename (with the full path) will be returned and displayed on TxtInp textbox.

Since the file is selected successfully, now it is time to do the real work…

Encryption

To do the encryption of the file, we will use the services provided by .NET platform.
The file encryption is carried out following these steps:

- Open and read the selected input file.

```
Dim sr As StreamReader = New StreamReader(TxtInp.Text)
Dim strInput As String = (sr).ReadToEnd()
sr.Close()
```

- Convert/encode the data read from the input file into Byte format

```
Dim byteArrayInput() As Byte = Encoding.Default.GetBytes(strInput)
```

- Create a filestream for the output (encrypted) file

```
Dim encFile As String = txtInp.Text + ".enc"
Dim fs As FileStream = New FileStream(encFile, FileMode.Create, FileAccess.Write)
```

- Use .NET services to create a cryptosystem that encrypts the input file (in Byte format) and store it in the output file.

```
des = New DESCryptoServiceProvider
Dim DESencrypt As ICryptoTransform = des.CreateEncryptor()
Dim DEScryptostream As CryptoStream = New CryptoStream(fs, DESencrypt,
CryptoStreamMode.Write)
DEScryptostream.Write(bytearrayinput, 0, bytearrayinput.Length)
DEScryptostream.Close()
fs.Close()
```

- To show the user that the file was encrypted successfully, a messagebox is used as follows:

```
MessageBox.Show("File is encrypted successfully")
```

Decryption

Similarly, to implement the decryption part, we will use the services provided by .NET platform. To do so, write the following code in "btnDec_Click" event sub:

- Open and read the selected input file.

```
Dim fsread As FileStream = New FileStream(TextBox1.Text, FileMode.Open, FileAccess.Read)
```

- Use the "des" DESCryptoServiceProvider created earlier to produce a cryptosystem that decrypts the chosen file.

```
Dim desdecrypt As ICryptoTransform = des.CreateDecryptor()
Dim cryptostreamDecr As CryptoStream = New CryptoStream(fsread, desdecrypt,
CryptoStreamMode.Read)
Dim decryptedFile As String = New StreamReader(cryptostreamDecr).ReadToEnd()
```

- Prepare the output file and write the decrypted data to that file

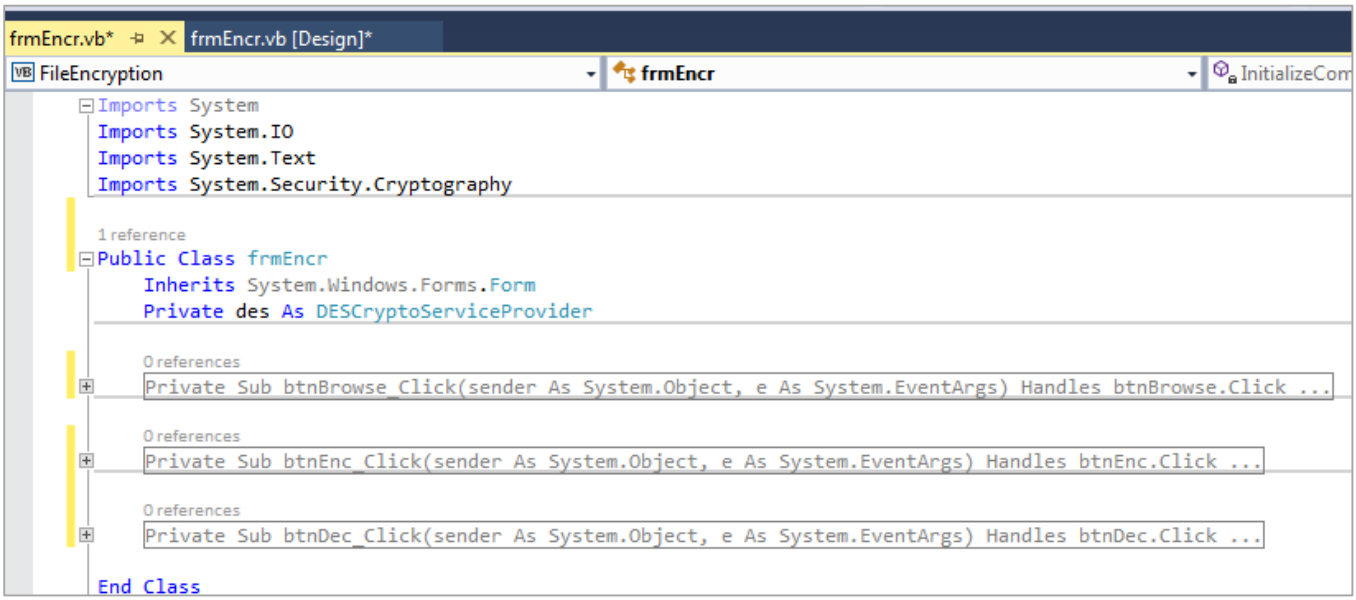
```
Dim fi As FileInfo = New FileInfo(TextBox1.Text)
Dim originalFile As String = TextBox1.Text.Substring(0, TextBox1.Text.Length -
fi.Extension.Length)
Dim fileWriter As StreamWriter = New StreamWriter(originalFile)
fileWriter.Write(decryptedFile)
fileWriter.Close()
```

- To show the user that the file was encrypted successfully, a messagebox is used as follows:

```
MessageBox.Show("File is decrypted successfully")
```

Final Product:

At the end of this session you should have the following codes:



The "btnBrowse_Click" sub should look like this:

```
0 references
Private Sub btnBrowse_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnBrowse.Click
    OFD1.ShowDialog()
    txtInp.Text = OFD1.FileName

End Sub
```

The "btnEnc_Click" sub should look like this:

```
Private Sub btnEnc_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnEnc.Click
    Dim sr As StreamReader = New StreamReader(txtInp.Text)
    Dim strInput As String = (sr).ReadToEnd()
    sr.Close()

    Dim byteArrayinput() As Byte = Encoding.Default.GetBytes(strInput)

    Dim encFile As String = txtInp.Text + ".enc"
    Dim fs As FileStream = New FileStream(encFile, FileMode.Create, FileAccess.Write)


    des = New DESCryptoServiceProvider
    Dim DESencrypt As ICryptoTransform = des.CreateEncryptor()
    Dim DEScryptostream As CryptoStream = New CryptoStream(fs, DESencrypt, CryptoStreamMode.Write)
    DEScryptostream.Write(byteArrayinput, 0, byteArrayinput.Length)
    DEScryptostream.Close()
    fs.Close()

    MessageBox.Show("File is encrypted successfully")

End Sub
```

The "btnDec_Click" sub should look like this:

```
Private Sub btnDec_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnDec.Click
    Dim fsread As FileStream = New FileStream(TextBox1.Text, FileMode.Open, FileAccess.Read)

    ' des = New DESCryptoServiceProvider
    Dim desdecrypt As ICryptoTransform = des.CreateDecryptor()
    Dim cryptostreamDecr As CryptoStream = New CryptoStream(fsread, desdecrypt, CryptoStreamMode.Read)
    Dim decryptedFile As String = New StreamReader(cryptostreamDecr).ReadToEnd()

    Dim fi As FileInfo = New FileInfo(TextBox1.Text)
    Dim originalFile As String = TextBox1.Text.Substring(0, TextBox1.Text.Length - fi.Extension.Length)
    Dim fileWriter As StreamWriter = New StreamWriter(originalFile)
    fileWriter.Write(decryptedFile)
    fileWriter.Close()

    MessageBox.Show("File is decrypted successfully")

End Sub
```

Question 1:

DES is a symmetric algorithm that needs one key for the encryption and decryption processes. Did we use a key in our coding? If Yes, what is the key used?

Question 2:

How can you do a similar program as above but using user-specific or custom key for encryption and decryption? What are the changes that you need to make in the above program to perform this task?