LAMPIRAN A

LISTING PROGRAM

***Form Main Program (Program Pengaman Data)**

```
Option Explicit
Dim LineOfText As String
Dim AllText As String
Dim Wrap As String
Dim s(0 To 255) As Integer 'S-Box
Dim kep(0 To 255) As Integer
Dim i As Integer, j As Integer
'For the file actions
Dim path As String
```

‘Program Inisialisasi RC4

```
Public Sub RC4ini(Pwd As String)

   Dim temp As Integer
   Dim A As Integer
   Dim B As Integer
   'Save Password in Byte-Array
   B = 0


   For A = 0 To 255
      B = B + 1


      If B > Len(Pwd) Then
         B = 1
      End If

      kep(A) = Asc(Mid$(Pwd, B, 1))
   Next A

   'INI S-Box


   For A = 0 To 255
      s(A) = A
   Next A
```

```
    B = 0

    'Mixing S-Box


    For A = 0 To 255
        B = (B + s(A) + kep(A)) Mod 256
        ' Swap( S(i),S(j) )
        temp = s(A)
        s(A) = s(B)
        s(B) = temp
    Next A

End Sub
```

‘Program untuk mendapatkan nilai k

```
Public Function EnDeCryptSingle(plainbyte As Byte) As Byte

    Dim temp As Integer, k As Integer
    Dim cipherby As Byte
    i = (i + 1) Mod 256
    j = (j + s(i)) Mod 256
    ' Swap( S(i),S(j) )
    temp = s(i)
    s(i) = s(j)
    s(j) = temp
    'Generate Keybyte k
    k = s((s(i) + s(j)) Mod 256)
    'Plaintextbyte xor Keybyte
    cipherby = plainbyte Xor k
    EnDeCryptSingle = cipherby
End Function
```

‘Open PlainText

```
Private Sub cmdBrowse_Click()
    Wrap$ = Chr$(13) + Chr$(10)
    AllText$ = ""
    dlgSourceFile.Filter = "Text files (*.TXT)|*.TXT|All files (*.*)|*.*"
    dlgSourceFile.ShowOpen
    If dlgSourceFile.FileName <> "" Then
    frmMain.MousePointer = 11
    Open dlgSourceFile.FileName For Input As #1
    On Error GoTo TooBig:    'set error handler
        Do Until EOF(1)         'then read lines from file
            Line Input #1, LineOfText$
```

```
        AllText$ = AllText$ & LineOfText$ & Wrap$
      Loop
      txtPlain.Text = ""
      txtPlain.Text = AllText$ 'display file
      txtSave.Text = dlgSourceFile.FileName 'display path
      txtPlain.Enabled = True

CleanUp:
      dlgSourceFile.FileName = ""
      frmMain.MousePointer = 0   'reset mouse
      Close #1                   'close file
   End If
   Exit Sub
TooBig:           'error handler displays message
   MsgBox ("The specified file is too large.")
   Resume CleanUp: 'then jumps to CleanUp routine
End Sub
```

‘Open CipherText

```
Private Sub cmdBrowse2_Click()
   Wrap$ = Chr$(13) + Chr$(10)
   AllText$ = ""
   dlgSourceCipher.Filter = "Cipher files (*.TXT.enc)|*.TXT.enc|All files
(*.*)|*.*"
   dlgSourceCipher.ShowOpen
   If dlgSourceCipher.FileName <> "" Then
   frmMain.MousePointer = 11
   Open dlgSourceCipher.FileName For Input As #1
   On Error GoTo TooBig:    'set error handler
      Do Until EOF(1)         'then read lines from file
         Line Input #1, LineOfText$
         AllText$ = AllText$ & LineOfText$ & Wrap$
      Loop
      txtCipher.Text = ""
      txtCipher.Text = AllText$ 'display file
      txtSave2.Text = dlgSourceCipher.FileName 'display path
      txtCipher.Enabled = True

CleanUp:
      dlgSourceCipher.FileName = ""
      frmMain.MousePointer = 0   'reset mouse
      Close #1                   'close file
   End If
   Exit Sub
TooBig:           'error handler displays message
```

```
   MsgBox ("The specified file is too large.")
   Resume CleanUp: 'then jumps to CleanUp routine
End Sub
```

‘Program pengecekan validasi dan digital signature

```
Private Sub cmdCekSignVal_Click()
Dim signcek As Long

If Text10.Text = "" Then
   MsgBox "Input the signature"
   Exit Sub
ElseIf txtPublikE.Text = "" Or txtPublikN.Text = "" Then
'txtPublikE.Text = "" Or txtPublikN.Text = "" Then
   MsgBox "Input your publik key"
   Exit Sub
End If

   Wrap$ = Chr$(13) + Chr$(10)
   AllText$ = ""
   CommonDialog3.Filter = "Text files (*.TXT)|*.TXT|All files (*.*)|*.*"
   CommonDialog3.ShowOpen
   If CommonDialog3.FileName <> "" Then
   frmMain.MousePointer = 11
   Open CommonDialog3.FileName For Input As #1
   On Error GoTo TooBig:    'set error handler
      Do Until EOF(1)         'then read lines from file
         Line Input #1, LineOfText$
         AllText$ = AllText$ & LineOfText$ & Wrap$
      Loop
      txtValSign.Text = ""
      txtValSign.Text = AllText$ 'display file
      txtValSign.Enabled = True
      signcek = pangkatmod(txtValSign.Text, txtPublikE.Text, txtPublikN.Text)
      Text9.Text = signcek

CleanUp:
      CommonDialog3.FileName = ""
      frmMain.MousePointer = 0   'reset mouse
      Close #1                'close file

   If Text9.Text = Text10.Text Then
      MsgBox "Data Verified", vbOKOnly, "ProjectRC4"
      Exit Sub
   Else
      MsgBox "Data is not Valid or Wrong Signature", vbOKOnly, "ProjectRC4"
```

```
        Exit Sub

    End If
    End If
    Exit Sub
TooBig:          'error handler displays message
    MsgBox ("This File is not Sign Document.")
    Resume CleanUp: 'then jumps to CleanUp routine


End Sub
```

‘Program Dekripsi

```
Private Sub cmdDecrypt_Click()
    Dim OldTimer2 As Single
    Dim inbyte As Byte
    Dim z As Long

    OldTimer2 = Timer
    'Set the Set-Box counter zero
    i = 0: j = 0
    'Ini the S-Boxes only once for a whole file


    If txtpwd2.Text = "" Then
        MsgBox "Enter Secret Key for Decipher"
        Exit Sub
    Else
        RC4ini (txtpwd2.Text)
    End If

    'Disable the Mousepointer
    MousePointer = vbHourglass
    path = txtSave2
    Open path For Binary As 1
    path = Left$(path, Len(path) - 4)
    Open path For Binary As 2


    For z = 1 To LOF(1)
        Get #1, , inbyte
        Put #2, , EnDeCryptSingle(inbyte)
    Next

    Close 1
```

```
    Close 2
    Label2.Caption = Timer - OldTimer2
    'Enable the Mousepointer
    MousePointer = vbDefault

End Sub
```

‘Program Enkripsi

```
Private Sub cmdEncrypt_Click()
    Dim oldtimer As Single
    Dim inbyte As Byte
    Dim z As Long
    oldtimer = Timer
    'Set the Set-Box Counter zero
    i = 0: j = 0
    'Ini the S-Boxes only once for a hole file

    If txtpwd.Text = "" Then
        MsgBox "Enter Secret Key for Encipher"
        Exit Sub
    Else
        RC4ini (txtpwd.Text)
    End If

    'Disable the Mousepointer
    MousePointer = vbHourglass
    path = txtSave
    Open path For Binary As 1
    Open path + ".enc" For Binary As 2


    For z = 1 To LOF(1)
        Get #1, , inbyte
        Put #2, , EnDeCryptSingle(inbyte)
    Next z

    Close 1
    Close 2
    Label1.Caption = Timer - oldtimer
    'Enable the Mousepointer
    MousePointer = vbDefault
End Sub
```

‘Program Generator Digital Signature

```
Private Sub cmdGen_Click()
```

```
Dim p As Long 'random prime
Dim q As Long 'second random prime that not equal to p
Dim n As Long 'p * q
Dim pi As Long '(p - 1)(q - 1)
Dim e As Long 'e that relatively prime to pi but less than pi
Dim d As Long 'd that d*e congruent to 1 mod pi
Dim i1 As Long 'counter

Dim c As Long
Dim temp1 As Long
Dim temp2() As Long ' temp dynamic array handler that hand selection of e
Dim temp3 As Long
Dim temp4 As Long
Dim temp5 As Long ' temp handler
Dim temp6 As Long ' temp handler 2


frmMain.MousePointer = 11
repeat:
   p = RdmPrime
   q = RdmPrime2

   'Trap handler if p = q
   If p = q Then
   GoTo repeat
   End If

   txt4.Text = p
   Text4.Text = q

   n = p * q

Text7.Text = n
cpyText7.Text = n
   pi = (p - 1) * (q - 1)

'search for e
c = pi - 1
ReDim temp2(c)

For e = 2 To (pi - 1)
   temp6 = gcd(pi, e)

   If temp6 = 1 Then
   temp2(c) = e
```

```
   c = c - 1
   End If

Next

'random selection of e
ulang:
   Randomize
   temp3 = Int((pi - 1) * Rnd)
   temp4 = temp2(temp3)
   If temp4 = 0 Or temp4 = Null Then
   GoTo ulang
   End If

'select e that is prime
For i1 = 2 To (Sqr(temp4))
temp5 = temp4 Mod i1
   If temp5 = 0 Then
     GoTo ulang
   End If
Next i1

Text5.Text = temp4

'determine d such that d*e congruent 1 mod pi and d > 0, d > e
d = Euclid(pi, temp4)
If d < temp4 Then
GoTo ulang
End If

Text6.Text = d

frmMain.MousePointer = 0
End Sub
```

‘Program Save PlainText yang sudah ditulis

```
Private Sub cmdSaveRaw_Click()

If txtRaw = "" Then
   MsgBox "Type your message"
   Exit Sub

Else

  CommonDialog1.Filter = "Text files (*.TXT)|*.TXT"
```

```
  CommonDialog1.ShowSave
  If CommonDialog1.FileName <> "" Then
    Open CommonDialog1.FileName For Output As #1
    Print #1, txtRaw.Text
    CommonDialog1.FileName = ""
    Close #1
  End If

End If

End Sub
```

‘Program Digital Signature nilai Validasi

```
Private Sub cmdValSign_Click()
Dim sign As Long
Dim Pal2 As Long
Dim pjgpesan As Long
Dim itung1 As Long
Dim itung2 As Long
Dim Pal() As Long

If Text6.Text = "" Then
   MsgBox "Click the generate button"
   Exit Sub
End If

pjgpesan = Len(txtPlain.Text)
ReDim Pal(pjgpesan)

   For itung1 = 0 To (pjgpesan - 1)
      Pal(itung1) = Asc(Mid(txtPlain.Text, itung1 + 1, 1))
   Next

If pjgpesan = 1 Then
Pal2 = Pal(0)
End If

If pjgpesan = 2 Then
Pal2 = Pal(0) Xor Pal(1)
End If

If pjgpesan = 3 Then
Pal2 = Pal(0) Xor Pal(1)
Pal2 = Pal2 Xor Pal(2)
End If
```

```
If pjgpesan > 3 Then

   Pal2 = Pal(0) Xor Pal(1)
   itung2 = 1

   Do

   Pal2 = Pal2 Xor Pal(itung2 + 1)
   itung2 = itung2 + 1

   Loop Until itung2 = pjgpesan

End If
sign = pangkatmod(((Pal2 ^ 2) Mod 251), Text6.Text, Text7.Text)
Text8.Text = sign
'Text10.Text = (Pal2 ^ 2) Mod 251

If Text8.Text = "" Then
      MsgBox "Error signing the plain document"
      Exit Sub
   Else
      CommonDialog2.Filter = "Text files (*.TXT)|*.TXT"
      CommonDialog2.ShowSave
         If CommonDialog2.FileName <> "" Then
         Open CommonDialog2.FileName For Output As #1
         Print #1, Text8.Text
         CommonDialog1.FileName = ""
         Close #1
         End If
      MsgBox "Document has been signed", vbOKOnly, "ProjectRC4"
End If
End Sub
```

‘Program me-load file ciphertext yang sudah didekripsi

```
Private Sub cmdView_Click()
Dim Pal2 As Long
Dim pjgpesan As Long
Dim itung1 As Long
Dim itung2 As Long
Dim Pal() As Long
Dim TextDeposit As String

   Wrap$ = Chr$(13) + Chr$(10)
   AllText$ = ""
```

```
    CommonDialog3.Filter = "Text files (*.TXT)|*.TXT"
    CommonDialog3.ShowOpen
    If CommonDialog3.FileName <> "" Then
    frmMain.MousePointer = 11
    Open CommonDialog3.FileName For Input As #1
    On Error GoTo TooBig:    'set error handler
       Do Until EOF(1)         'then read lines from file
          Line Input #1, LineOfText$
          AllText$ = AllText$ & LineOfText$ & Wrap$
       Loop
       TextDeposit = AllText$
       txtDecipherM = ""
       If TextDeposit <> "" Then
          txtDecipherM.Text = "File Loaded"
       Else
          txtDecipherM.Text = "File Not Loaded"
       End If
       'txtDecipherM.Text = AllText$ 'display file
       'txtDecipherM.Enabled = True

pjgpesan = Len(TextDeposit)
ReDim Pal(pjgpesan)

    For itung1 = 0 To (pjgpesan - 1)
       Pal(itung1) = Asc(Mid(TextDeposit, itung1 + 1, 1))
    Next

If pjgpesan = 1 Then
Pal2 = Pal(0)
End If

If pjgpesan = 2 Then
Pal2 = Pal(0) Xor Pal(1)
End If

If pjgpesan = 3 Then
Pal2 = Pal(0) Xor Pal(1)
Pal2 = Pal2 Xor Pal(2)
End If

If pjgpesan > 3 Then

    Pal2 = Pal(0) Xor Pal(1)
    itung2 = 1
```

```
   Do

   Pal2 = Pal2 Xor Pal(itung2 + 1)
   itung2 = itung2 + 1

   Loop Until itung2 = pjgpesan

End If
Text10.Text = (Pal2 ^ 2) Mod 251

CleanUp:
      CommonDialog3.FileName = ""
      frmMain.MousePointer = 0   'reset mouse
      Close #1                   'close file
   End If
   Exit Sub

TooBig:           'error handler displays message
   MsgBox ("The specified file is too large.")
   Resume CleanUp: 'then jumps to CleanUp routine

End Sub
```

‘Program menampilkan menu About

```
Private Sub mnuAbout_Click()
frmAbout.Show
End Sub
```

‘Program Exit

```
Private Sub mnuExitItem_Click()
End
End Sub
```

‘Program menampilkan menu How To Use

```
Private Sub mnuHow_Click()
frmHow.Show
End Sub
```

‘Program Function

```
Public Function DecimalToBinary(DecimalNum As Long) As String
Dim tmp As String
Dim n1 As Long

n1 = DecimalNum
```

```
tmp = Trim(Str(n1 Mod 2))
n1 = n1 \ 2

Do While n1 <> 0
tmp = Trim(Str(n1 Mod 2)) & tmp
n1 = n1 \ 2
Loop

DecimalToBinary = tmp
End Function

Function Euclid(ByVal nilai1, ByVal nilai2) As Long
Dim mex As Long
Dim bex As Long
Dim A1 As Long
Dim A2 As Long
Dim A3 As Long
Dim Qex As Long
Dim T1 As Long
Dim T2 As Long
Dim T3 As Long
Dim B1 As Long
Dim B2 As Long
Dim B3 As Long
Dim hasil As Long

mex = nilai1
bex = nilai2

A1 = 1
A2 = 0
A3 = mex

B1 = 0
B2 = 1
B3 = bex

itung:

If B3 = 0 Then
hasil = 0
GoTo selesai
End If

If B3 = 1 Then
```

```
hasil = B2
GoTo selesai
End If

Qex = A3 \ B3

T1 = A1 - Qex * B1
T2 = A2 - Qex * B2
T3 = A3 - Qex * B3

A1 = B1
A2 = B2
A3 = B3

B1 = T1
B2 = T2
B3 = T3

GoTo itung

selesai:
Euclid = hasil

End Function

Function gcd(ByVal p, ByVal q) As Long
Dim A11 As Long
Dim B11 As Long
Dim R11 As Long

   A11 = p
   B11 = q

label:
   If B11 = 0 Then
   gcd = A11
   Else
   R11 = A11 Mod B11
   A11 = B11
   B11 = R11
   GoTo label
   End If

End Function
```

```
Function RdmPrime() As Long
Dim iRandom As Long ' holds random long result
Dim i2 As Long ' checkprime loop counter
Dim temp2a As Long 'swap var

Const iLowerBound = 30
Const iUpperBound = 300

   Randomize

110
   iRandom = (Int((iUpperBound - iLowerBound + 1) * Rnd() + iLowerBound))
'trap handler

If iRandom = 0 Or iRandom = 1 Then
GoTo 110
End If

 'check number
 For i2 = 2 To (Sqr(iRandom))
   temp2a = iRandom Mod i2
   If temp2a = 0 Then
     GoTo 110
   End If
 Next i2

   RdmPrime = iRandom

End Function

Function RdmPrime2() As Long
Dim iRandom2 As Long ' holds random long result
Dim y As Long 'checkprime loop counter
Dim holder As Long 'swap var

  Randomize

120
   iRandom2 = (Int(Asc(Date) Xor 255 * Rnd))
'trap handler

If iRandom2 = 0 Or iRandom2 = 1 Then
GoTo 120
End If
```

```
'check number
For y = 2 To (Sqr(iRandom2))
   holder = iRandom2 Mod y
   If holder = 0 Then
     GoTo 120
   End If
Next y

   RdmPrime2 = iRandom2

End Function
Function pangkatmod(ByVal num1, ByVal num2, ByVal num3) As Long
Dim a22 As Long
Dim b22 As Long
Dim n22 As Long
Dim nilaimod As Long
Dim nilaic As Long
Dim nilaid As Long
Dim nilaii As Long
Dim nilaik As Long
Dim naik As Long
Dim barray() As Variant
Dim decbin As Variant

a22 = num1
b22 = num2
n22 = num3

decbin = DecimalToBinary(b22)
nilaic = 0
nilaid = 1
nilaik = Len(decbin)
ReDim barray(nilaik)
naik = 1

For nilaii = nilaik - 1 To 0 Step -1
barray(nilaii) = Mid(decbin, naik, 1)
naik = naik + 1
nilaic = 2 * nilaic
nilaid = (nilaid * nilaid) Mod n22
   If barray(nilaii) = 1 Then
      nilaic = nilaic + 1
      nilaid = (nilaid * a22) Mod n22
   End If
Next
```

```
pangkatmod = nilaid

End Function
```

***Form About**

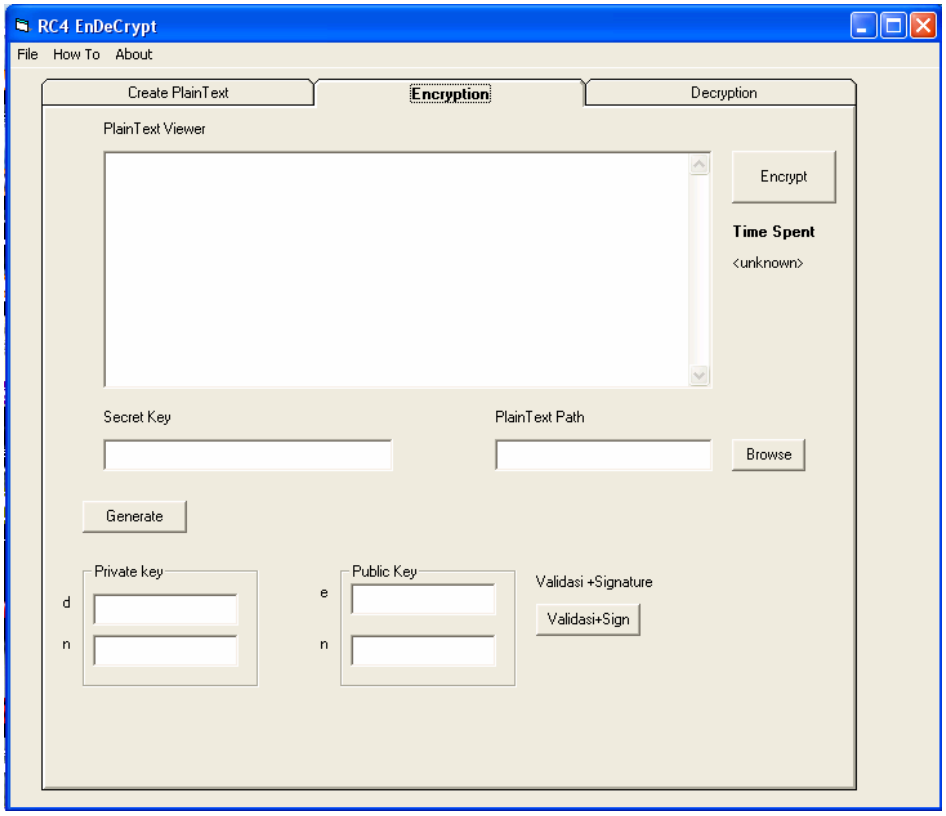
```
Private Sub cmdOK_Click()
Unload Me
End Sub
```

***Form How**

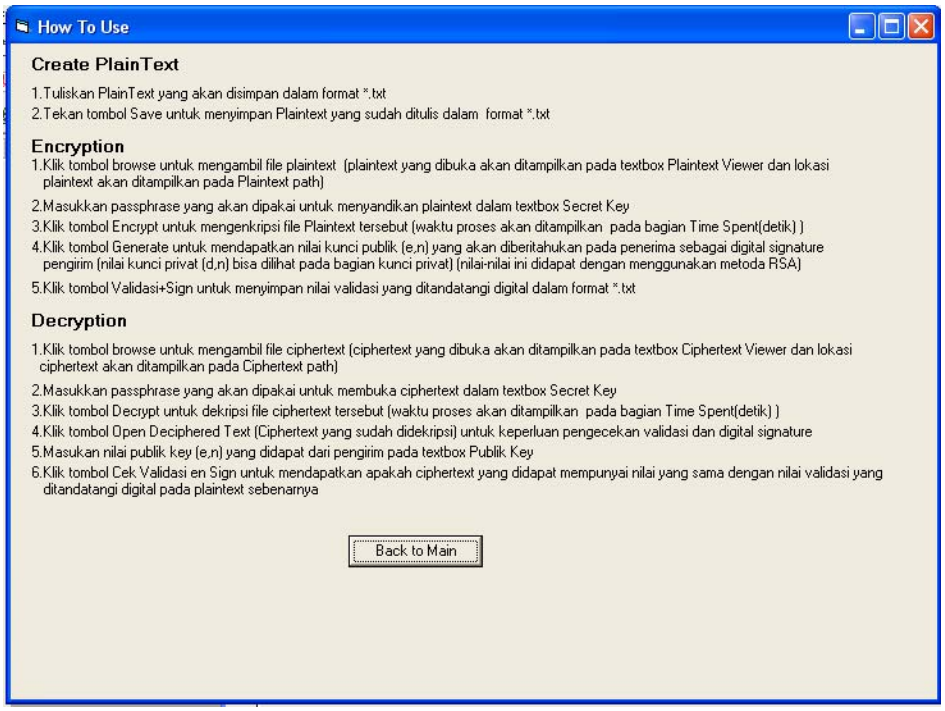
```
Private Sub cmdBack_Click()
Unload Me
End Sub
```

LAMPIRAN B

TAMPILAN PROGRAM PENGAMAN DATA

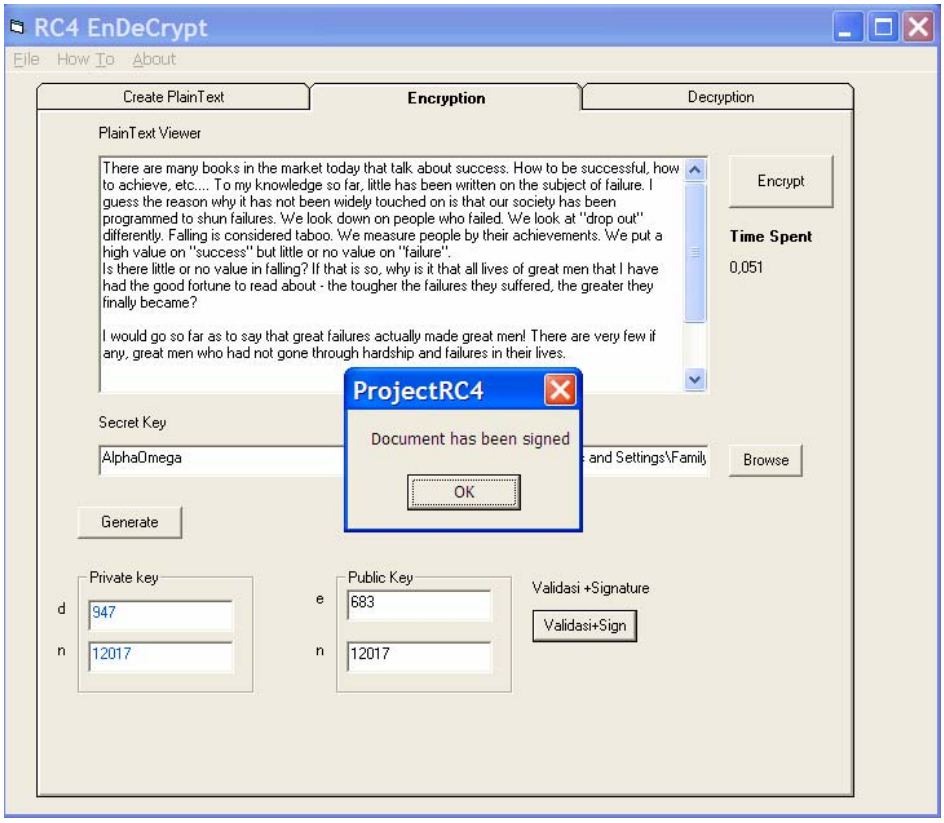


Tampilan Awal Program Pengaman Data

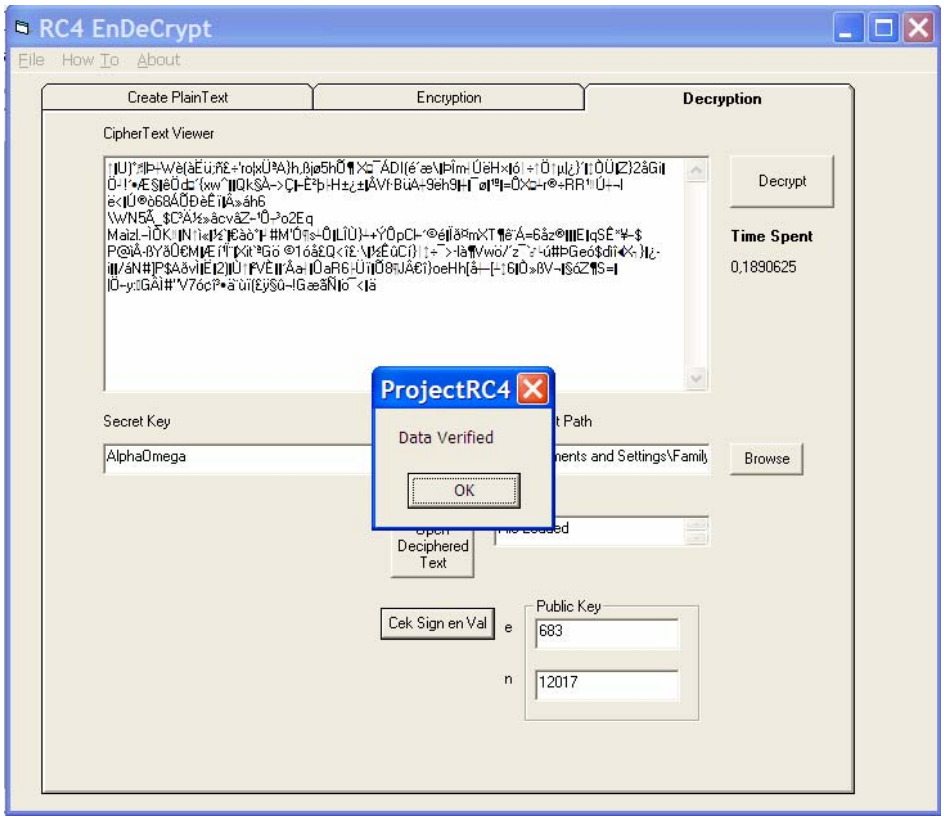


Tampilan Menu How To

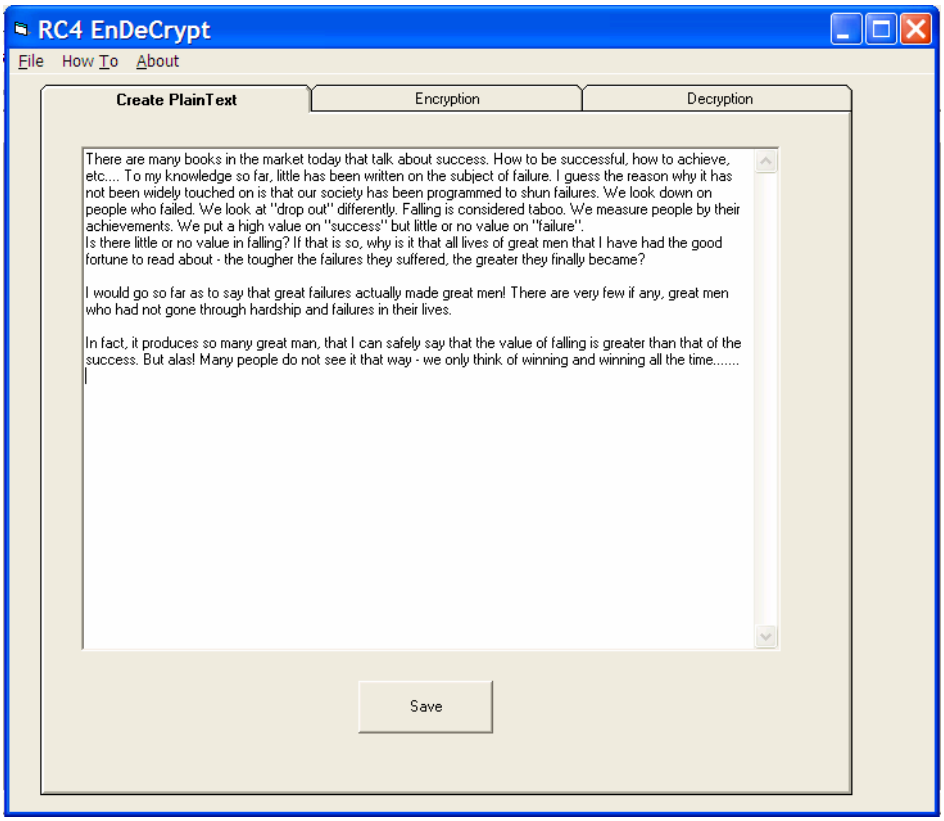
Tampilan Menu About



Tampilan Menu Program Enkripsi



Tampilan Menu Dekripsi



Tampilan Menu Create Plaintext