Kriptografi Menggunakan VB.NET

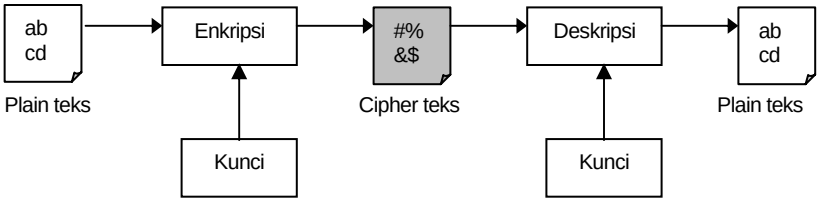
Ario Suryo Kusumo
ario_sk@hotmail.com

Kriptografi adalah ilmu atau seni untuk untuk menjaga keamanan pesan. Ketika suatu pesan ditransfer dari suatu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat di-*scramble*/diacak atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain.

Tujuan kriptografi adalah:

- **Confidentiality.** Untuk melindungi identitas pemakai atau isi pesan agar tidak dapat dibaca oleh orang lain yang tidak berhak.
- **Data Integrity.** Untuk melindungi pesan agar tidak diubah oleh orang lain.
- **Authentication**. Untuk menjamin keaslian pesan.
- **Non repudiation**. Membuktikan suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim pesan tersebut.

Dalam dunia kriptografi, pesan yang akan dirahasiakan disebut plain teks. Pesan yang sudah diacak disebut cipher teks. Proses untuk mengkonversi plain teks menjadi cipher teks disebut enkripsi. Proses untuk mengembalikan plain teks dari cipher teks disebut deskripsi. Algoritma kriptografi (ciphers) adalah fungsi-fungsi matematika yang digunakan untuk melakukan enkripsi dan deskripsi. Diperlukan kunci yaitu kode untuk melakukan enkripsi dan deskripsi.



Gambar 1 Proses enkripsi dan deskripsi

Ada dua macam tipe kunci enkripsi yaitu: kunci simetris dan kunci asimetris. Algoritma simetris menggunakan kunci yang sama untuk mengenkrip dan mendeskrip. Algoritma asimetris menggunakan dua kunci, kunci publik untuk enkripsi dan kunci pribadi untuk melakukan deskripsi. Contoh cara kerjanya, jika Rangga ingin mengirim pesan kepada Cinta, maka Rangga akan mengenkripsi pesannya menggunakan kunci publik dari Cinta. Ketika Cinta menerima pesan dari Rangga, maka Cinta akan menggunakan kunci pribadinya untuk mendeskripsi pesan dari Rangga. (jadi, Ada Apa Dengan Cinta? ☺)

Kriptografi dalam VB.NET

Microsoft menyediakan kumpulan class kriptografi yang merupakan perluasan dari layanan/services kriptografi pada Windows CryptoAPI.

Kumpulan class kriptografi terdapat dalam namespace System.Security.Cryptography, dan dapat dibagi menjadi empat divisi yaitu:

Divisi	Penjelasan
Encryption Algorithms (Algoritma Enkripsi)	Sekumpulan class yang dapat digunakan untuk mengimplementasikan algoritma simetris, asimetris dan hash.
Helper Classes (Class-class penolong)	Class-class yang digunakan untuk menghasilkan angka acak, melakukan konversi, interaksi dengan penyimpanan Crypto API, dan melakukan enkripsi menggunakan model berbasis *stream*/aliran data.
X.509 Certificates (Sertifikasi X.509)	Class-class yang terdapat pada namespace System.Security.Cryptography.X509, dapat digunakan untuk memberikan sertifikasi digital.
XML Digital Signatures (Tanda tangan digital XML)	Class-class yang terdapat pada namespace System.Cryptography.Xml, dapat digunakan untuk memberikan tanda tangan digital dalam dokumen XML.

Tabel 1 Komponen Kriptografi

Tipe enkripsi yang disediakan dalam .NET antara lain:

Metode Enkripsi	Tipe Umum	Class .NET
DES (Data Encryption Standard)	Simetris (kunci privat)	DESCryptoServiceProvider
RC2 (RSA Data Security, Inc.)	Simetris (kunci privat)	RC2CryptoServiceProvider
Rijndael	Simetris (kunci privat)	RijndaelManaged
TripleDES (menggunakan tiga enkripsi DES)	Simetris (kunci privat)	TripleDESCryptoServiceProvider
DSA (Digital Signature Algorithm)	Asimetris (kunci publik)	DSACryptoServiceProvider
RSA (dari tiga nama penemunya Rivest, Shamir, dan Adelman)	Asimetris (kunci publik)	RSACryptoServiceProvider

Tabel 2 Tipe enkripsi dalam .NET

Anda tidak perlu tahu bagaimana cara kerja metode enkripsi secara rinci karena rumit, tetapi jika Anda akan memilih metode enkripsi, ada tiga faktor yang perlu dipertimbangkan yaitu:

- Tingkat kesulitan untuk meng-*crack*/menembus pesan yang dienkrip menggunakan suatu metode enkripsi.
- Performa dari metode enkripsi misalnya kecepatan dalam melakukan enkripsi dan deskripsi.
- Keamanan dari kunci.

Menggunakan Class-class Enkripsi .NET

Class-class enkripsi disimpan dalam namespace System.Security.Cryptography, dan untuk menggunakannya pada aplikasi, Anda harus melakukan referensi memakai pernyataan Imports berikut:

```
Imports System.Security
Imports System.Security.Cryptography
```

Class enkripsi akan berkerja sama dengan class *streaming*/aliran data kriptografi yang disebut **CryptoStream.** CrypoStream akan mengikat objek kriptografi agar dapat digunakan bersama, artinya suatu output dari satu objek kriptografi dapat secara langsung diarahkan sebagai input dari objek kriptografi lainnya tanpa perlu menyimpan hasil output ke objek perantara. Hal ini akan menambah performa secara signifikan jika mengenkrip atau mengdeskrip data yang ukurannya besar.

Misalnya untuk enkripsi, langkah-langkahnya sebagai berikut:

1. Byte-byte yang masuk berasal dari *input stream*/aliran data input (misalnya file yang tidak dienkrip dalam disk).
2. Byte-byte diberikan ke stream enkripsi, yang berhubungan dengan output stream (contohnya, file yang akan menangani enkripsi data).

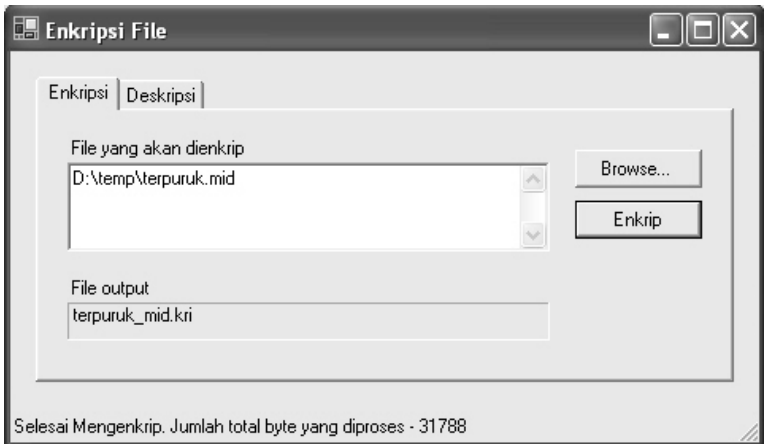
3. Stream enkripsi akan mengenkrip byte-byte dan secara otomatis akan menempatkan hasilnya dalam output stream yang berhubungan.

Membuat Program Enkripsi File

Membuat program enkripsi file menggunakan metode *DES (Data Encryption Standard*) dimana kuncinya simetri. Kita akan menggunakan class DESCryptoServiceProvider.

Kebanyakan algoritma simetris membutuhkan dua array bytes terpisah yang digunakan dalam proses enkripsi. Pertama berupa kunci, pada latihan ini akan dimasukkan pemakai dalam bentuk password, untuk DES berukuran 8 bytes. Kedua disebut *initialization vector* (IV) berupa array bytes yang ukurannya sama dengan kunci. IV gunanya untuk menghindari seseorang melakukan *reverse engineer* (rekayasa balik) agar mendapat kunci, karena IV akan mengenkrip blok pertama data yang biasanya berisi header pesan umum termasuk kunci. Dalam program ini pemakai hanya diminta memasukkan kunci saja, IV nilainya diatur secara otomatis berisi kebalikan dari kunci menggunakan fungsi StrReverse.

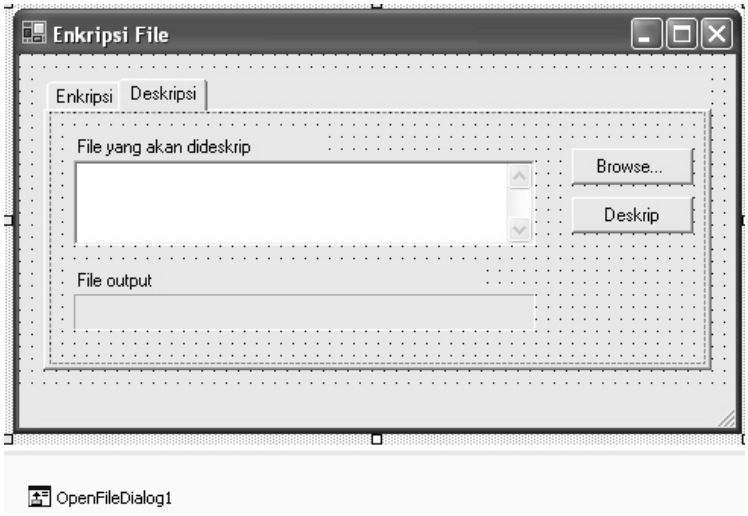
Pada waktu melakukan deskripsi jika pemakai salah dalam memasukkan password/kunci, akan muncul pesan error dan aplikasi akan ditutup.



Gambar 3 Program Enkripsi File saat dijalankan

Langkah untuk membuat program sebagai berikut:

1. Jalankan VB.NET dan di jendela New Project, pilih Template dengan Windows Application dan beri Name dengan “Enkripsi File”.
2. Tambahkan komponen OpenFileDialog ke form dengan cara klik ganda.
3. Tambahkan kontrol TabKontrol ke form. Klik properti TabPages dan pada kotak dialog TabPage Collection Editor klik tombol Add dua kali. Atur properti Text dari members TabPage1 dengan “Enkripsi” dan properti Text dari TabPage2 dengan “Deskripsi”.
4. Tambahkan kontrol lainnya ke form dan atur propertinya. Isi tab Enkripsi seperti Gambar 3 dan tab Deskripsi Gambar 4.



Gambar 4 Form program Enkripsi File tab Deskripsi.

Properti:

Objek	Properti	Pengaturan
Form1	Text	Enkripsi File
StatusBar1	Text	
OpenFileDialog1	Name	OpenFileDialog1
Objek di Tab Enkripsi		
Label1	Text	File yang dienkrip
TextBox1	ScrollBars Text Multiline	Vertical True
Label2	Text	File Output
Label3	BorderStyle Text Name	Fixed3D lblOutputEn
Button1	Text	Browse…
Button2	Text	Enkrip
Objek di Tab Deskripsi		
Label4	Text	File yang dideskrip
TextBox2	ScrollBars Text Multiline	Vertical True
Label5	Text	File Output
Label6	BorderStyle Text Name	Fixed3D lblOutputDe
Button3	Text	Browse…
Button4	Text	Deskrip

Tabel 3 Properti program Enkripsi File

5. Tambahkan kode sebagai berikut:

Kode:

```
'Sumber MSDN Library, "Tales from the Crypto", Billy Hollis

Imports System.IO
Imports System.Security
Imports System.Security.Cryptography
Public Class Form1
    Inherits System.Windows.Forms.Form
    Private Enum CryptoAction
        actionEncrypt = 1
        actionDecrypt = 2
    End Enum

Windows Form Designer generated code
Private password As String

Private Function GetKeyByteArray(ByVal sPassword As String) _
        As Byte()
    Dim TempByte(7) As Byte
    sPassword = sPassword.PadRight(8)   ' pastikan 8 hrf

    Dim iCharIndex As Integer
    For iCharIndex = 0 To 7
        TempByte(iCharIndex) = Asc(Mid$(sPassword, _
                iCharIndex + 1, 1))
    Next

    Return TempByte
End Function

Private Sub Button1_Click(ByVal sender As System.Object, _
        ByVal e As System.EventArgs) Handles Button1.Click
    ' Membuka file untuk dienkrip
    OpenFileDialog1.Title = "Pilih file untuk dienkrip"
    OpenFileDialog1.Filter = "All files (*.*)|*.*"

    If OpenFileDialog1.ShowDialog() = DialogResult.OK Then
        TextBox1.Text = OpenFileDialog1.FileName
        Button2.Enabled = True
        NamaFileDienkrip()
    End If
End Sub

Private Sub NamaFileDienkrip()
    ' Ekstrak nama file dari path penuh
    Dim Posisi As Integer = 0
    Dim t As Integer = 0
    While TextBox1.Text.IndexOf("\"c, t) <> -1
        Posisi = TextBox1.Text.IndexOf("\"c, t)
        t = Posisi + 1
    End While
    ' Merancang nama file output
    ' Dengan pola: namafile_ekstensi_kri
    ' Contoh: "Cucak Rowo.mp3" -> "Cucak Rowo_mp3.kri"
    Dim FileOutput As String = TextBox1.Text.Substring _
            ((Posisi + 1))
    FileOutput = FileOutput.Replace("."c, "_"c)
    lblOutputen.Text = FileOutput + ".kri"
End Sub
```

```
    Private Sub Button2_Click(ByVal sender As System.Object, _
            ByVal e As System.EventArgs) Handles Button2.Click
        ‘ Menampilkan kotak dialog password
        Dim passForm As New Form2
        If passForm.ShowDialog() = DialogResult.OK Then
            password = passForm.Password
            MengenkripFile()
        End If
    End Sub

    Private Sub MengenkripFile()
        Dim byteKey() As Byte
        byteKey = GetKeyByteArray(password)
        Dim byteIV() As Byte
        byteIV = GetKeyByteArray(StrReverse(password))

        EnkripatauDeskrip(TextBox1.Text, _
                          lblOutputen.Text, _
                          byteKey, byteIV, _
                          CryptoAction.actionEncrypt)
    End Sub

    Private Sub Button3_Click(ByVal sender As System.Object, _
                ByVal e As System.EventArgs) Handles Button3.Click
        OpenFileDialog1.Title = "Pilih file untuk dideskrip"
        OpenFileDialog1.Filter = "File krip (*.kri)|*.kri"
        If OpenFileDialog1.ShowDialog() = DialogResult.OK Then
            TextBox2.Text = OpenFileDialog1.FileName
            Button3.Enabled = True

            NamaFileDideskrip()
         End If
    End Sub

    Private Sub NamaFileDideskrip()
        ‘ Ekstrak nama file dari path penuh
        Dim Posisi As Integer = 0
        Dim t As Integer = 0

        While TextBox2.Text.IndexOf("\"c, t) <> -1
            Posisi = TextBox2.Text.IndexOf("\"c, t)
            t = Posisi + 1
        End While

        Dim FileOutput As String = TextBox2.Text.Substring(0, _
                TextBox2.Text.Length - 4)
        FileOutput = FileOutput.Substring((Posisi + 1))
        lblOutputDe.Text = FileOutput.Replace("_"c, "."c)
    End Sub

    Private Sub Button4_Click(ByVal sender As System.Object, _
            ByVal e As System.EventArgs) Handles Button4.Click
        ‘ Menampilkan kotak dialog password
        Dim passForm As New Form2
        If passForm.ShowDialog() = DialogResult.OK Then
            password = passForm.Password
            MendeskripFile()
        End If
    End Sub

    Private Sub MendeskripFile()
        Dim byteKey() As Byte
        byteKey = GetKeyByteArray(password)
```

```
        Dim byteIV() As Byte
        byteIV = GetKeyByteArray(StrReverse(password))

        EnkripatauDeskrip(TextBox2.Text, _
                          lblOutputDe.Text, _
                          byteKey, byteIV, _
                          CryptoAction.actionDecrypt)
    End Sub



    Private Sub EnkripatauDeskrip(ByVal sInputFile As String, _
        ByVal sOutputFile As String, ByVal byteDESKey() As Byte, _
        ByVal byteDESIV() As Byte, ByVal Direction As CryptoAction)

        ‘ Membuat file stream untuk menangani file input dan
        ‘ output.
        Dim fsInput As New FileStream(sInputFile, _
                FileMode.Open, FileAccess.Read)
        Dim fsOutput As New FileStream(sOutputFile, _
                FileMode.OpenOrCreate, FileAccess.Write)
        fsOutput.SetLength(0)

        ‘ Variabel yang diperlukan selama proses
        ‘ enkrip dan deskrip

        ‘ Menahan suatu blok dari byte untuk proses
        Dim byteBuffer(4096) As Byte
        ‘ Menjalankan hitungan byte yang dienkrip
        Dim nBytesProcessed As Long = 0
        Dim nFileLength As Long = fsInput.Length
        Dim iBytesInCurrentBlock As Integer
        Dim desProvider As New DESCryptoServiceProvider
        Dim csMyCryptoStream As CryptoStream
        Dim sArah As String

        Try
            ‘ Atur enkripsi atau deskripsi
            Select Case Direction
                Case CryptoAction.actionEncrypt
                    csMyCryptoStream = New CryptoStream(fsOutput, _
                       desProvider.CreateEncryptor _
                       (byteDESKey, byteDESIV), _
                       CryptoStreamMode.Write)
                    sArah = "Mengenkrip"

                Case CryptoAction.actionDecrypt

                    csMyCryptoStream = New CryptoStream(fsOutput, _
                        desProvider.CreateDecryptor _
                        (byteDESKey, byteDESIV), _
                        CryptoStreamMode.Write)
                    sArah = "Mendeskrip"

            End Select

            StatusBar1.Text = "Mulai " + sArah + " ..."

            ‘ Membaca dari file input kemudian mengenkrip
            ‘ atau mendeskrip dan menulis ke file output
            While nBytesProcessed < nFileLength
                iBytesInCurrentBlock = fsInput. _
                        Read(byteBuffer, 0, 4096)
```

```
                csMyCryptoStream.Write(byteBuffer, 0, _
                        iBytesInCurrentBlock)
                nBytesProcessed = nBytesProcessed + _
                        CLng(iBytesInCurrentBlock)
                StatusBar1.Text = sArah + _
                        " dalam proses - Byte yang diproses - " + _
                        nBytesProcessed.ToString
            End While
            StatusBar1.Text = "Selesai " + sArah + _
                         ". Jumlah total byte yang diproses - " + _
                                nBytesProcessed.ToString
            csMyCryptoStream.Close()
            fsInput.Close()
            fsOutput.Close()
        Catch varError As Exception
            MessageBox.Show("Password deskrip " _
                      & "tidak cocok dengan enkrip!", _
                      "Password tidak cocok")
            Me.Close()
         End Try

    End Sub

    End Class
```

Catatan:
Dalam kode Private Sub EnkripatauDeskrip, bagian pertama adalah membuat objek file *stream/*aliran data dengan nama fsInput dan fsOutput untuk menerima input dari file yang dibaca dan menghasilkan output berupa file baru. Berikutnya terdapat beberapa deklarasi variabel yaitu:

- byteBuffer, suatu array byte yang digunakan untuk memroses blok data. byteBuffer pengisiannya dengan cara membaca file input kemudian diberikan ke objek CryptoStream untuk dienkripsi. Kode berikutnya adalah loop (perulangan) melalui file input, menarik blok sebesar 4096 byte dan ditempatkan dalam byteBuffer.
- nBytesProcessed, untuk menghitung banyaknya angka total bytes dari file input yang diproses hingga kini.
- nFileLength, merupakan panjang dari file input.
- iBytesInCurrentBlock, jumlah dari bytes yang diproses dalam suatu iterasi dari perulangan. Tiap iterasi dilakukan pada 4096 byte data kecuali iterasi yang terakhir. Pada iterasi terakhir yang diproses adalah sisa jumlah byte dalam blok file terakhir (umumnya kurang dari 4096).
- desProvider, dihubungkan ke CryptoStream untuk menyediakan fungsionalitas enkripsi/deskripsi yang akan kita gunakan.
- csMyCryptoStream, merupakan objek CryptoStream yang digunakan untuk enkripsi atau deskripsi.
- sDirection, merupakan nilai dari CryptoAction (actionEncrypt atau actionDecrypt) untuk operasi yang ingin kita jalankan.

Bagian berikutnya adalah suatu Select Case yang akan mengatur enkripsi atau deskripsi, tergantung pada apa yang akan kita lakukan dengan eksekusi dari fungsi. DESCryptoServiceProvider dapat melakukan enkripsi atau deskripsi menggunakan metode CreateEncryptor atau CreateDecryptor. Metode tersebut digunakan untuk instansiasi (menaruh nilai pada suatu variabel) objek CryptoStream yang akan kita gunakan, dengan nama csMyCryptoStream. Objek csMyCryptoStream juga perlu untuk mengetahui stream apa yang

digunakan untuk output, baik enkripsi maupun deskripsi, stream fsOutput menentukan untuk tujuan ini selama instantiasi dari csMyCryptoStream.

Kita juga akan mengatur suatu teks yang berisi nilai enkripsi atau deskripsi yang akan ditampilkan sebagai pesan dalam status bar.

Akhirnya, kita akan membahas bagian kode yang secara aktual melakukan enkripsi atau deskripsi. Loop While akan membaca data dari file input satu blok pada suatu waktu. Kemudian blok tersebut ditulis ke csMyCryptoStream menggunakan metode Write. csMyCryptoStream secara otomatis akan melakukan enkripsi atau deskripsi dan menulis hasilnya ke ke file stream yang diambil yaitu fsOutput. Selanjutnya kita akan meng-update jumlah total bytes berjalan yang diproses ke pesan di status bar dan diulang kembali ke blok lainnya.

Setelah loop selesai, kita akan meng-update teks di status bar, menutup objek stream dan selesai.

6. Tambahkan sebuah form baru dengan klik menu Project > Add Windows Form. Pilih templates dengan Windows Form dan klik tombol Open. Tambahkan kontrol ke form, atur properti dan ketik kode.

Gambar 5 Form pengisian password

Properti:

Objek	Properti	Pengaturan
Form2	Text	Memasukkan Password
Label1	Text	Password
TextBox1	Text PasswordChar	 *
Label2	Text	Konfirmasi Password
TextBox2	Text PasswordChar	 *
Button1	Text DialogResult	OK OK
Button2	Text DialogResult	Batal Cancel

Tabel 4 Properti Form2 program Enkripsi File

Kode:

```
Private Sub button1_Click(ByVal sender As Object, ByVal e _
        As System.EventArgs) Handles Button1.Click
  ‘ Cek kedua password harus cocok atau
```

```
      'password harus ada isinya dan >= 8
      If TextBox1.Text.Length < 8 OR _
               TextBox1.Text <> TextBox2.Text Then
          MessageBox.Show("Password yang Anda masukkan " _
            & "kurang dari 8 karakter, tidak cocok atau kosong!", _
                 "Password salah!")
          Me.DialogResult = DialogResult.None
      End If
     End Sub 'button1_Click

    Public ReadOnly Property Password() As String
            Get
                Return TextBox1.Text
            End Get
        End Property
    End Class 'Form2
```

Sumber:

Pustaka MSDN, artikel "*Tales from the Crypto*", oleh Billy Hollis