BAB III

ANALISIS MASALAH DAN RANCANGAN PROGRAM

III.1 Analisis

Sistem yang sudah ada saat ini adalah sistem yang dimana sebuah aplikasi Text Editor hanyalah sebagai media pengetikan *Source Code* pemograman pada umumnya. Secara keseluruhan sistem yang ada pada saat ini belum mencukupi atau belum ada pengembangan suatu fasilitas tambahan yang digunakan oleh aplikasi text editor.Aplikasi Text Editor plus ini memanfaatkan media pemograman menggunakan software pemograman Visual Basic 2005 atau Visual Basic 2008, yaitu salah satu aplikasi berbasis windows yang menjadi antar muka dengan pengguna (user).

III.2 Analisa Kebutuhan Sistem

Pada tahap analisa kebutuhan kriptografi DES, RC2 dan Rijndael serta fasilitas tambahannya pada aplikasi teks editor ini, dalam perancangannya dan implementasinya membutuhkan perangkat lunak dan perangkat keras.

Adapun jenis perangkat lunak dan perangkat keras yang dipakai adalah sebagai berikut :

1. Perangkat Keras
    a. Mikro processor Pentium IV Core I3 2.30 Ghz
    b. Memory 2 Gb
    c. VGA Card 2 Giga Byte

2. Perangkat Lunak
    a. Sistem Operasi Windows 7 Home Basic 32 Byte Versi 4.4
    b. Microsoft Visual Studio 2010

III.3 Strategi Pemecahan Masalah

Dalam aplikasi Text editor yang beredar sebelumnya belum terdapat metode atau fasilitas yang bisa digunakan atau dimanfaatkan sebagi keperluan lain selain hanya sebagai media penulisan *Source* program pada umumnya. Dalam hal ini menjadi masalah tersendiri dimana pengguna tidak bisa merasakan fungsi dari kelebihan dari aplikasi text editor itu sendiri melainkan hanya sebagai media pengetikan *source code.* Hal ini menjadi masalah yang dihadapi penulis dalam mengembangkan sebuah aplikasi Text editor yang bersifat multifungsi yang dapat digunakan sebagai media lain atau fungsi lain selain sebagai media pengetikan yang umumnya tidak tersedia pada text editor.

Ada beberapa strategi pemecahan masalah yang akan diterapkan pada perancangan text editor plus ini diantaranya:

1. Mengumpulkan Teori

    Dimana dalam proses perancangan ini sebelumnya perlu diketahui analisis atau teori dari masalah yang akan di terapkan dalam proses perancangan.

2. Merancang Program

    Perancangan program ini adalah dengan membuat suatu rancangan tampilan dan fungsi yang akan diterapkan dalam penggunaan metode metode yang akan digunakan.

3. Mengimplementasikan Perancangan Program

   Implementasi perancangan program adalah dimana program yang telah dirancang di implemetasikan dengan tujuan sebenarnya dari proses rancangan yang telah di buat.

III.4 Perancangan Analisa masalah Sistem

Dalam analisa dan perancangan perangkat lunak teks editor dengan fasilitas tambahan dan metode kriptografi DES, RC2 dan Rijndael yang di implementasikan, penulis menggunakan flowchart sebagai alat bantu perancangan analisa masalah sistem dan sebuah form sebagai media interaksi user dengan perangkat lunak.

III.5 Perancangan

Adapun rancangan sistem yang akan dibangun penulis adalah dengan membandingkan terlebih dahulu terhadap sistem yang lama. Rancangan sistem yang penulis lakukan adalah menyeleksi algoritma sistem yang akan digunakan sebagai alat bantu perancangan. Berikut adalah algoritma yang akan penulis rancang dengan menggunakan Cryptografi Net Framework.

III.6 Algoritma Enkripsi Deskripsi Dengan Crytografi Net FrameWork

Didalam aplikasi teks editor yang dirancang penulis, penulis menggunakan Cryptografi Net Frame Work sebagai media pemrosesan Proses Kriptografi. Di dalam modul itu kita tidak memproses data secara langsung, tetapi hanya

mengubah teks menjadi aliran data kriptografi (KriptoStream), yaitu inputstrem, kemudian memasukkannya ke dalam kelas Cryptografi Net Framework untuk di proses berdasarkan metode enkripsi yang kita inginkan. Selanjutnya output hasil proses tersebut (OutputStrim) diambil oleh kelas modul kita menjadi output kelas modul.

Berikut ini adalah tahap demi tahap proses algoritma enkripsi dan dekripsi menggunakan Cryptografi net Framework adalah sebagai berikut:

```
Imports System.IO
```

Berfungsi sebagai pengimpor objek IO untuk mendapatkan object memory stream karena kita akan menampung keluaran dari object Cryptografi Net Framework dalam memory stream

```
Imports System.Text
```

Berfungsi mengimpor object text dari object System karena kita memerlukan object tersebut dalam hal mengubah text yang kita masukkan menjadi data byte. Yang dapat menjadi plaintext adalah bentuk data byte.

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

Berfungsi mengimpor object Cryptografi karena objek ini yang menjadi tempat mengubah plainteks menjadi ciphertext atau sebaliknya.

```
Enum MetodeEnskripsi
        DES
        RC2
        Rijndael
    End Enum
```

Berfungsi sebagai pembuat variable jenis baru yang bernama MetodeEnkripsi yang terdiri atas item DES,RC2 dan Rijndael. Dengan variable ini kita dapat

mengatur supaya hanya ada ada 3 pilihan tersebut , seperti halnya variable jenis boolean yang hanya ada 2 pilihan.

```
Private Function GetKeyByteArray(ByVal password As String)
As Byte()
        Dim tmpbyte(7) As Byte
        password = password.PadRight(8)
        For i As Integer = 0 To 7
            tmpbyte(i) = Asc(Mid$(password, i + 1, 1))
        Next
        Return tmpbyte
    End Function
```

Berfungsi sebagai pembuat prosedur fungsi GetKeyByteArray yang berfungsi mengubah nilai string password ke dalam aray byte dengan pembatasan ukuran password 8 karakter.

```
Public Function Enskrip(ByVal plainText As String, ByVal password
As String, Optional ByVal Metode As MetodeEnskripsi =
MetodeEnskripsi.DES) As String
        On Error Resume Next
```

Berfungsi membuat prosedur fungsi enkrip yang mengubah plaintext menjadi ciphertext, dengan metode enkripsi default DES.

```
Dim bytekey() As Byte = GetKeyByteArray(password)
Dim byteIV() As Byte =
GetKeyByteArray(StrReverse(password))
Dim ToEncrypt As Byte() = Encoding.UTF8.GetBytes(plainText)
Dim Encryptor As ICryptoTransform
```

Algoritma diatas menjelaskan bahwa semua input yang talah di masukkan di ubah menjadi byte.

```
Select Case Metode
        Case MetodeEnskripsi.DES
             Dim Provider As New DESCryptoServiceProvider
             Encryptor = Provider.CreateEncryptor(bytekey,byteIV)
            Case MetodeEnskripsi.RC2
                Dim Provider As New RC2CryptoServiceProvider
```

```
                Encryptor = Provider.CreateEncryptor(bytekey, byteIV)
            Case Else
                byteIV = Encoding.ASCII.GetBytes("1234567890123456")
                Dim bSaltValue As Byte() = Encoding.ASCII.GetBytes("12")
                Dim pdbPassword As New PasswordDeriveBytes(password,
bSaltValue, "SHA1", 2)
                bytekey = pdbPassword.GetBytes(256 / 8)
                Dim Provider As New RijndaelManaged()
                Encryptor = Provider.CreateEncryptor(bytekey, byteIV)
        End Select
```

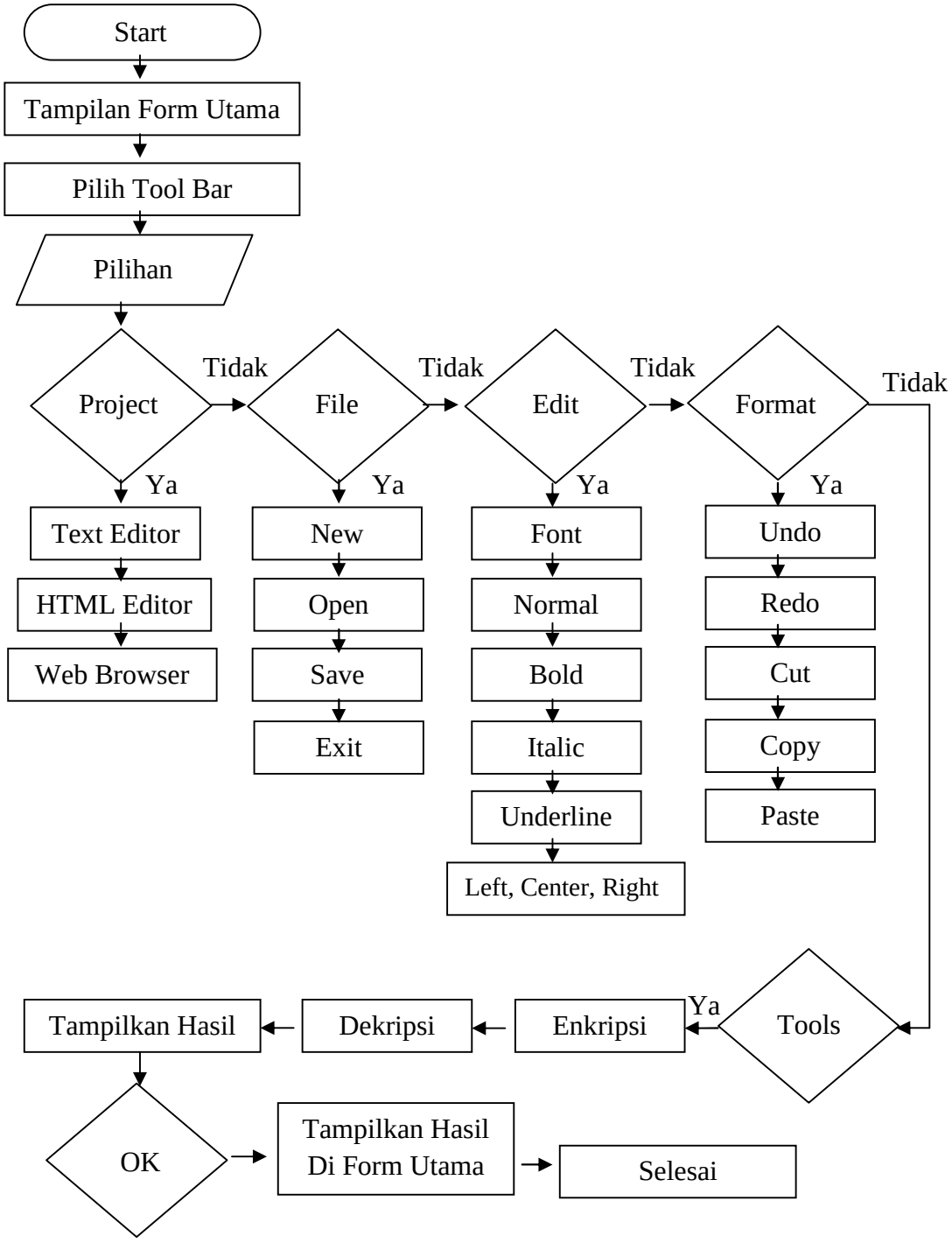
Algoritma di atas adalah proses pemilihan metode untuk menentukan provider, yaitu objeck sevice cryptpgrafi yang akan di gunakan. Selanjutnya dari provider tersebut di isi nilai tranform enkripsinyamengguanakan data password dalam bentuk data byte.

```
Dim msEncrypt As New MemoryStream()
        Dim csEncrypt As New CryptoStream(msEncrypt, Encryptor,
CryptoStreamMode.Write)

        csEncrypt.Write(ToEncrypt, 0, ToEncrypt.Length)
        csEncrypt.FlushFinalBlock()

        Dim encrypted As Byte() = msEncrypt.ToArray()

        msEncrypt.Close()
        csEncrypt.Close()

        Return Convert.ToBase64String(encrypted)
    End Function
```

Selanjutnya algoritma diatas membuat memory stream untuk kemudian dijadikan input objeck CryptoStream sebagai tempat menampung data pemrosesan enkripsi. Object tersebut terus menulis hingga akhir data dalam memory stream. Selanjutnya data dari memory stream tersebut diubah kembali mejadi data string (bukan byte) dan menjadi keluaran dari prosedur fungsi ini.

III.7 Flowchart Algoritma Sistem Cryptografi Net Framework

Berikut ini adalah tampilan flowchart sistem cryptografi net framework adalah sebagai berikut:

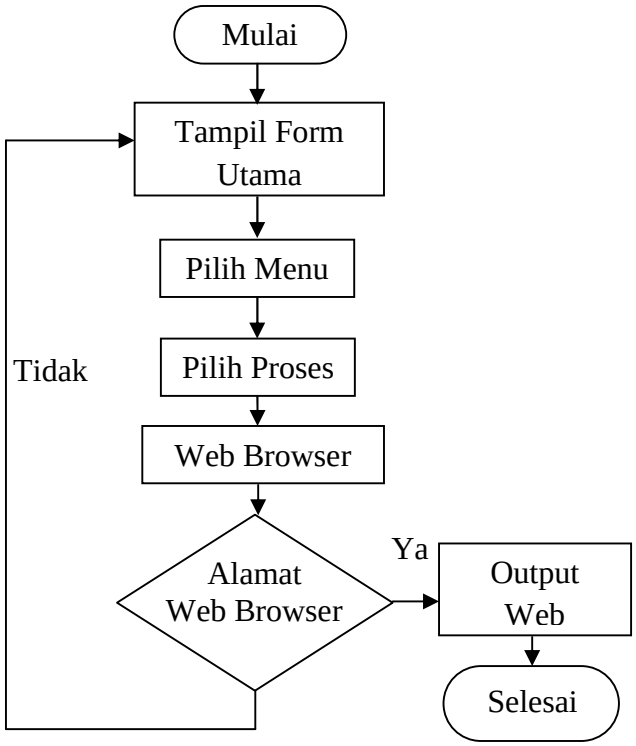


Gambar III.1 Flowchart Ringkas Sistem Cryptografi secara Keseluruhan

III.8 Fasilitas Web Browser

Web Browser atau internet browser adalah sebuah aplikasi perangkat lunak untuk melintasi, mengambil, dan menyajikan sumber informasi di World Wide Web (www). Sumber informasi diidentifikasi dengan Uniform Resource Identifier (URL) termasuk sebuah halaman Web, gambar, video, atau bagian lain dari konten web.

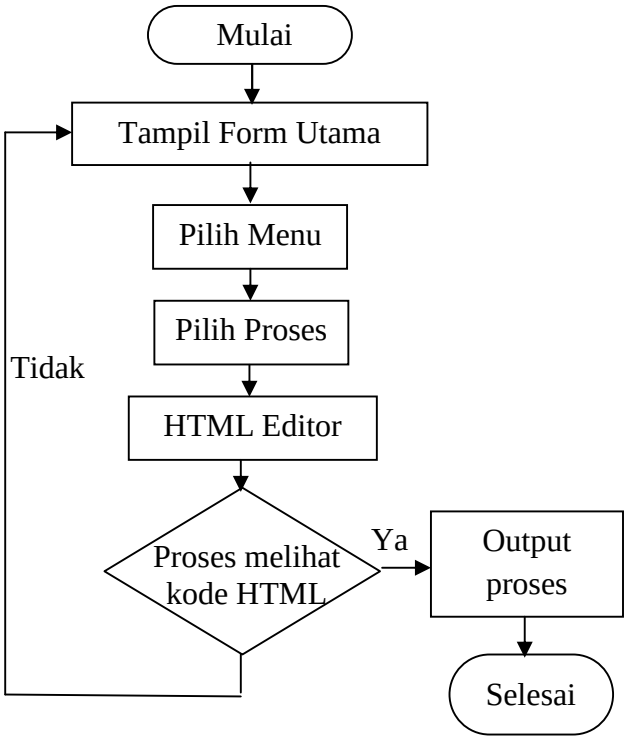
Dalam perancangan Teks Editor ini penulis menambahkan sebuah fasilitas lain yang belum ada sebelumnya yaitu Web Browser. Dengan adanya Web Browser di dalam aplikasi teks editor ini akan menjadi manfaat bagi user untuk membuka situs secara langsung tanpa harus berpindah keluar ke aplikasi web browser yang sudah ada sebelumnya. Berikut ini dijabarkan skema tampilan proses pada aplikasi teks editor dengan web browser:



Gambar III.2 Proses Web Browser Dalam Aplikasi

III.9 Fasilitas HTML Editor

Fasilitas lain yang terdapat pada apalikasi yang penulis rancang ini adalah fasilitas melihat kode HTML secara langsung tanpa harus menyimpan dahulu halaman Web Site nya. Dengan falilitas tambahan yang terdapat pada aplikasi ini pengguna dapat dengan mudah melihat kode HTML sebuah Web site dengan melaui beberapa proses yang disediakan pada aplikasi berikut. Berikut ini adalah tampilan diagram proses pada fasilitas melihat kode HTML.



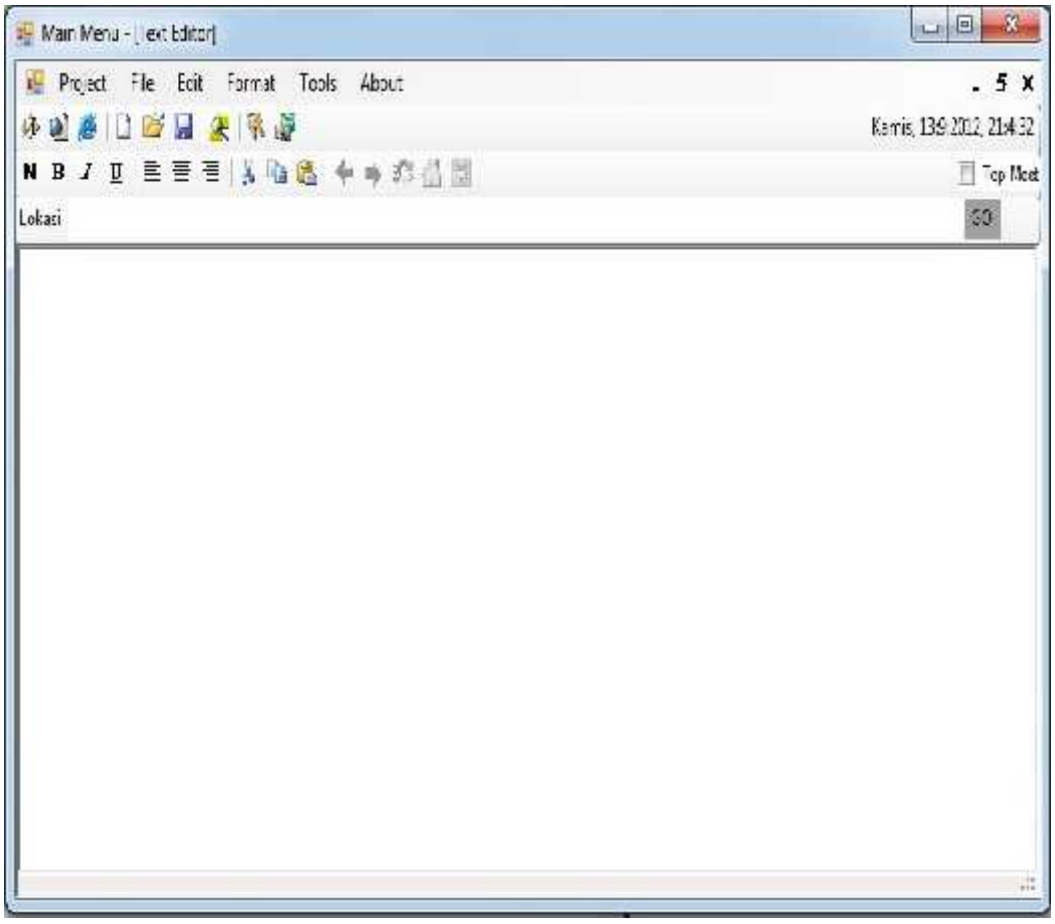
Gambar III.3 Proses Fasilitas HTML Editor Pada Aplikasi

III.10 Perancangan Antar Muka

Antar muka perangkat lunak Perancangan Aplikasi Text Editor Plus Dengan Fasilitas Web Browser Menggunakan Metode Enkripsi DES, RC2 dan Rijndael yang penulis rancang terdiri dari sebuah form.

1. **Rancangan Form Utama yang terdiri dari beberapa fungsi Menu Bar.**

   Form ini berisikan beberapa metode dan fungsi dari fasiliatas teks editor, yakni fasilitas HTML editor, Web Browser, Teks Editor, Enkripsi dan Dekripsi dengan metode DES, RC2 dan Rijndael, Capture, dan Waktu. Adapun bentuk rancangan form Utama seperti terlihat pada gambar III.13.



Gambar III.4 Rancangan Form Utama