PERANGKAT LUNAK PENGAMANAN DATA MENGGUNAKAN ALGORITMA MESSAGE DIGEST-5 (*MD-5*)

Sastya Hendri Wibowo[1*]
[1]Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Bengkulu
Jl. Bali Bengkulu
*e-mail : sastiahendriwibowo@gmail.com

Abstrak

Penelitian ini berjudul perangkat lunak pengamanan data menggunakan algoritma Message-Digest-5 atau MD-5. Adapun rumusan masalah yang diangkat dalam penelitian ini adalah bagaimana membuat perangkat lunak yang dapat digunakan untuk mengenkripsi dan dekripsi data dalam suatu folder, serta bagaimana mengimplemtasikan algoritma Message-Digest atau MD5 kedalam pengamanan suatu data dalam folder atau direktori. Batasan masalah dalam penelitian ini adalah algoritma yang digunakan adalah Message Digest atau MD5, data yang akan di enkripsi dan di dekripsi adalah data yang terdapat atau tersimpan pada suatu folder atau direktori. Tujuan dari penelitian adalah penerapan algoritma Message Digest-5 atau MD-5 pada keamanan data yang terdapat pada suatu folder atau direktori, data yang tersimpan dalam folder dapat di enkripsi dan didekripsi. Manfaat penelitian adalah Perangkat lunak ini dapat digunakan untuk mengamankan data yang terdapat pada suatu folder atau direktori tertentu dari pihak yang tidak bertanggung jawab sehingga isi dan kerahasiaan dari data tersebut terjaga. Metode pengumpulan data yang dipakai adalah studi pustaka dan lab research. Hasil akhir dari perangkat lunak yang dibuat akan di uji cobakan dengan menggunakan metode blackbox.

Kata kunci : *Kriptografi, Enkripsi, Dekripsi*

1. PENDAHALUAN

Komputer merupakan alat pengolah dan penyimpanan data, data yang diolah tidak hanya data dalam bentuk karakter tapi ada juga data yang berformat suara atau gambar. Data yang telah melalui proses pengolahan data oleh komputer akan tersimpan didalam media penyimpanan baik yang ada didalam komputer seperti hardisk ataupun dalam media lain sepert flashdisk, hardisk ekternal.

Data yang tersimpan kedalam media penyimpanan biasanya disimpan kedalam suatu folder atau direktori dan dikelompokkan sehingga dapat mudah untuk mencari. Disamping itu juga data yang tersimpan dalam media penyimpanan sering hilang atau dibuka oleh pihak-pihak tertentu yang tidak bertanggung jawab, sehingga dapat merugikan sekali bagi pemilik data tersebut, untuk itu diperlukan suatu pengamanan data menggunakan algoritma pengamanan data.

Algoritma Message Digest-5 atau MD-5 merupakan kriptografi dengan 128 – bit nilai hash. Ditentukan dalam RFC 1321, Message Digest-5 atau MD-5 telah digunakan dalam berbagai jenis aplikasi keamanan, dan juga sering digunakan untuk memeriksa integritas file sehingga algoritma Message Digest-5 atau MD-5 dapat menjaga keamanan data dari pengguna-pengguna (user) yang tidak bertanggung jawab. Sebuah hash MD-5 biasanya dinyatakan sebagai 32-digit heksadesimal nomor.

Algoritma Message Digest-5 atau MD-5 yang dirancang oleh Profesor Ronald L.Rivest merupakan algoritma massage digest atau kadang juga dikenal dengan hash function yaitu suatu algoritma yang inputnya berupa sebuah pesan yang panjangnya tidak tertentu, dan menghasilkan keluaran sebuah message digest dari pesan inputnya dengan panjang tepat 128 bit. Password MD-5 merupakan salah satu perlindungan kepada user dalam pengamanan data yang berada dalam sebuah komputer karena sebuah password adalah kunci yang sangat berharga bagi kita yang sering melakukan aktifitas yang berhubungan dengan perkantoran atau instasi tertentu.

1.1 Rumusan Masalah

a. Bagaimana membuat perangkat lunak yang dapat digunakan untuk mengenkripsi data
b. Bagaimana membuat perangkat lunak yang dapat digunakan untuk mendekripsi data
c. Bagaimana menerapkan algoritma Message Digest-5 atau MD-5 dalam pengamanan data yang tersimpan dalam suatu folder atau direktori

1.2 Batasan Masalah

a. Algoritma yang digunakan adalah Message Digest-5 atau MD-5
b. Data yang akan di enkripsi adalah data yang terdapat atau tersimpan dalam suatu folder atau direktori
c. Data yang akan di dekripsi adalah data yang terdapat atau tersimpan dalam suatu folder atau direktori

1.3 Tujuan Penelitian

a. Penerapan algoritma Message Digest-5 atau MD-5 pada keamanan data yang terdapat atau tersimpan pada suatu folder atau direktori
b. Data yang terdapat atau tersimpan dalam folder dapat di enkripsi
c. Data yang terdapat atau tersimpan dalam folder dapat di dekripsi

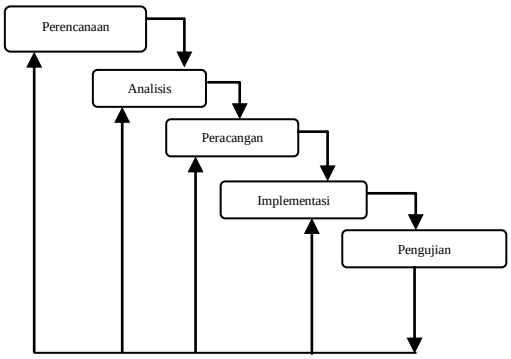
1.4 Manfaat Penelitian

Perangkat lunak ini dapat digunakan untuk mengamankan data yang terdapat pada suatu folder atau direktori terntu dari pihak yang tidak bertanggung jawab sehingga isi dan kerahasiaan dari data tersebut terjaga

2. METODOLOGI PENELITIAN

2.1 Model Pengembangan Sistem

Model pengembangan sistem yang dipakai yaitu *Classic Life Cycle* atau *Waterfall Model*, yang mencakup :



Gambar 1. Model Pengembangan Sistem Waterfall

1. Perencanaan
   Pada tahapan *perencanaan* ini bertujuan untuk mengarahkan pengembang agar sesuai dengan sistem yang akan dibuat, kemudian membatasi apa yang boleh dan tidak boleh dilakukan pada pembuatan sistem. Dalam tahapan ini ada tugas-tugas yang harus dijalankan antara lain membuat daftar calon atau kandidat *perencanaan*, memahami konteks sistem, memahami *requirement* fungsional dan non fungsional dan membuat validasinya.
2. Analisis
   Pada tahapan analisis ini bertujuan untuk mendapatkan pemahaman secara keseluruhan tentang sistem yang akan dikembangkan berdasarkan dari masukan calon pengguna. Kemudian untuk memodelkan sistem yang nyata dengan penekanan pada apa yang harus dilakukan bukan pada bagaimana melakukannya. Hasil utama dari analisis adalah pemahaman sistem seutuhnya sebagai persiapan menuju ke tahap perancangan *(design).*
   Pada penelitian ini adalah penerapkan algoritma Message Digest-5 kedalam suatu perangkat lunak yang dibuat menggunakan bahasa pemrograman Visual Basic 6, proses yang dilakukan terdiri dari Enkripsi dan Dekripsi.
3. Perancangan
   Pada tahapan ini bertujuan untuk menentukan bentuk sistem arsitektur yang memenuhi semua *perencanaan*, kemudian untuk memahami isu pada *perencanaan* non fungsional dan batasan teknologi, membuat abstraksi yang tak terlihat pada implementasi sistem dan menyediakan visualisasi implementasi.
4. Implementasi
   Setelah melalui tahapan *perencanaan*, *analisis* dan *perancangan*, maka sebuah sistem siap untuk diimplementasikan. Dalam tahapan implementasi ada beberapa tugas yang dijalankan

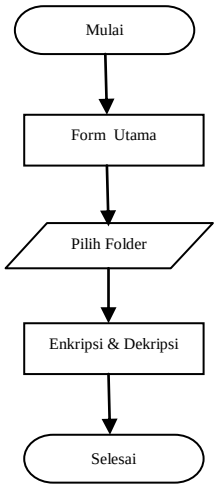
diantaranya mengimplementasikan desain dalam komponen-komponen *source code, script, executable* dan sebagainya, kemudian menyempurnakan arsitektur dan mengintegrasikan komponen-komponen (mengkompile dan link ke dalam satu atau lebih *executable*) untuk integrasi dan *testing* system

5. Pengujian
   Pada umumnya, dimanapun ada hasil implementasi, maka terdapat sebuah pengujian atau *testing*. Pengujian ini dilakukan pada setiap pembangunan, yaitu : Pengujian dilakukan dengan prosedur Black-box.

3. HASIL DAN PEMBAHASAN

3.1 Flowchart Enkripsi dan Dekripsi

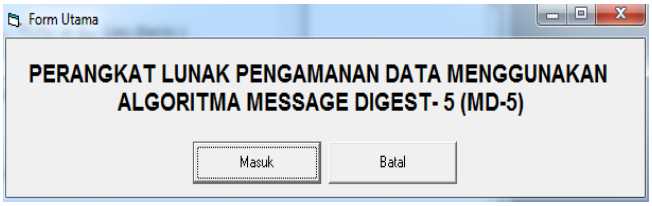
Flowchart merupakan alur dari suatu program, gambar dibawah menggambarkan alur dari perangkat lunak yang dijalankan.



Gambar 2. Flowchart Enkripsi dan Dekripsi

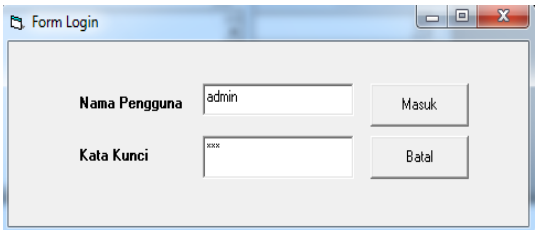
3.2 Tampilan Antar Muka Perangkat Lunak

3.2.1 Form Utama



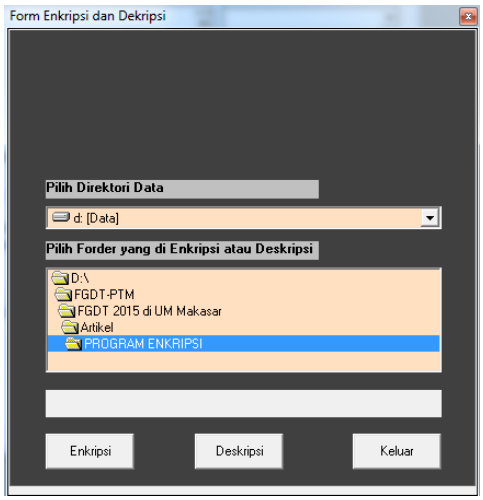
Gambar 3. Form Utama

3.2.2 Form Login



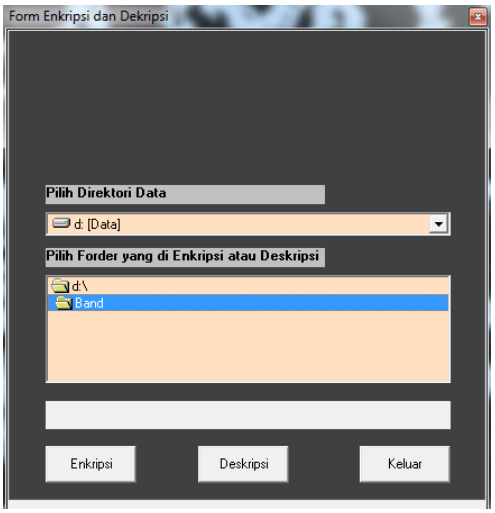
Gambar 4. Form Login

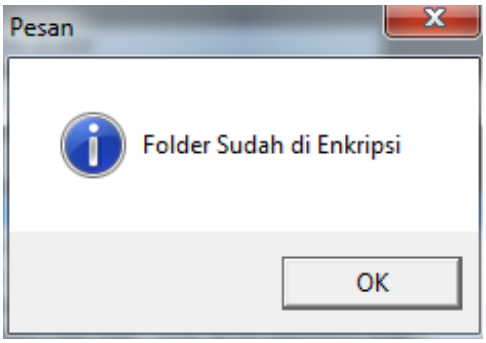
3.2.3 Form Enkripsi dan Dekripsi

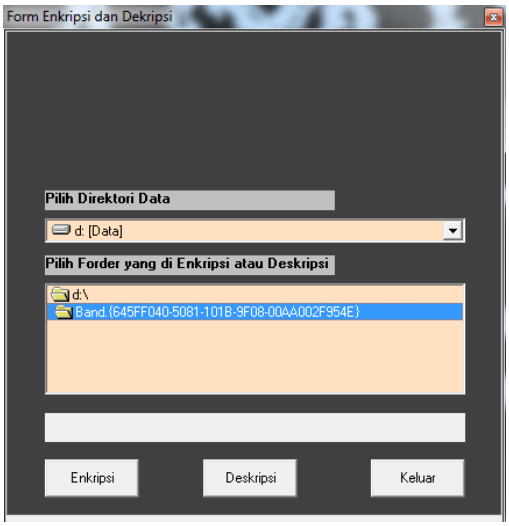


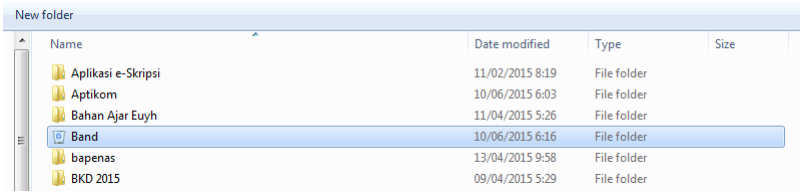
Gambar 5. Form Enkripsi dan Dekripsi

3.2.4 Proses Enkripsi





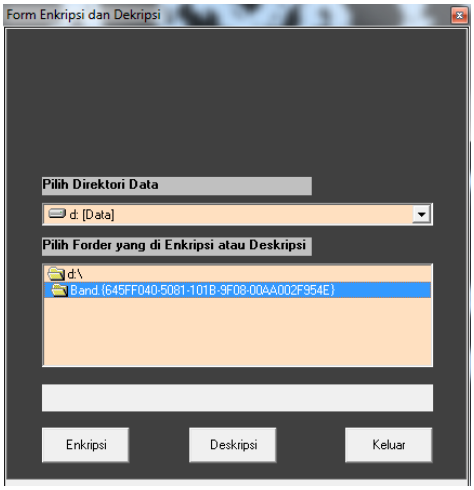


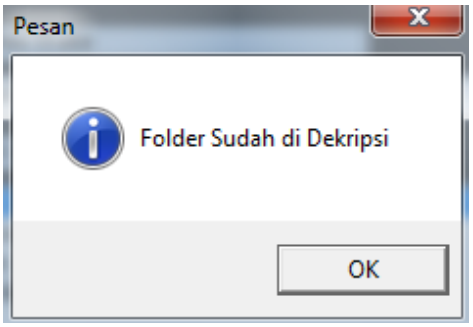


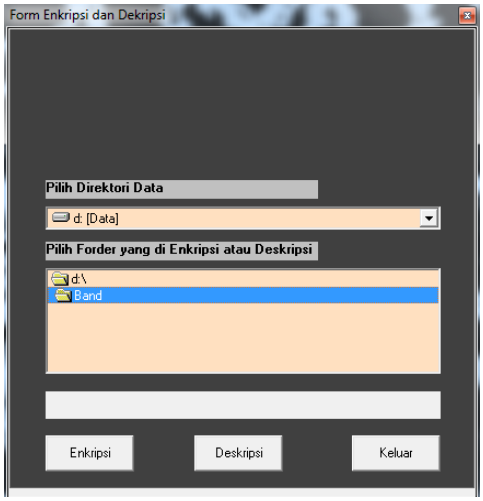

```
Private Sub Command1_Click()
On Error GoTo Err
   Dim Path As String
   Dim Data As String
   Dim File As String
   Dim md5 As String
   Dim FileName As String
   md5 = ".{645FF040-5081-101B-9F08-00AA002F954E}"
   Path = dirDir.Path
   Data = Mid$(Path, InStrRev(Path, "\") + 1, Len(Path))
   File = Left$(Path, Len(Path) - Len(Data))
   If Not UCase$(Path) = UCase$(WindowsDirectory) _
   And Not UCase$(Data) = UCase("desktop") Then
      FileName = File & Data & md5
      Name dirDir.Path As FileName
      dirDir.Path = File
      MsgBox "Folder Sudah di Enkripsi", vbApplicationModal + vbInformation, "Pesan"
   Else
      MsgBox "Folder Cannot be Locked.", vbApplicationModal + vbCritical, "Pesan"
   End If
Err:
   Exit Sub
End Sub
```

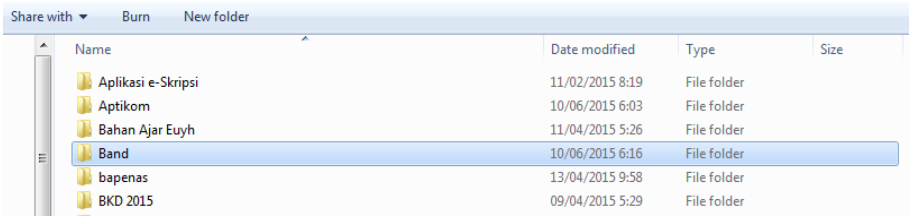
Gambar 6. Proses Enkripsi

3.2.5 Proses Dekripsi










```
Private Sub Command2_Click()
On Error GoTo Err
    Dim Path As String
    Dim Temp As String
    Dim Data As String
```

```
    Dim File As String
    Dim md5 As String
    Dim FileName As String
    Path = dirDir.Path
    Temp = Mid$(Path, InStrRev(Path, "\") + 1, Len(Path))
    Data = Left$(Temp, InStr(Temp, ".{") - 1)
    File = Left$(Path, Len(Path) - Len(Temp))
    FileName = File & Data
    Name dirDir.Path As FileName
    dirDir.Path = File
    MsgBox "Folder Sudah di Dekripsi", vbApplicationModal + vbInformation, "Pesan"
Err:
    Exit Sub
End Sub
```

Gambar 7. Proses Dekripsi

3.3 Pengujian Sistem

Tabel 1. Hasil Pengujian Perangkat Lunak

No	Sasaran	Keluaran	Status
1	Uji Form Utama	Tombol Masuk dan Tombol Batal	Baik
2	Uji Form Login	Tombol Masuk dan Tombol Batal	Baik
3	Uji Form Enkripsi dan Dekripsi	Tombol Enkripsi dan Dekripsi	Baik
4	Proses Enkripsi	• Pilih data dalam folder, tombol proses enkripsi dan tampilan kotak pesan • Algoritma MD-5 yang telah di konversi dalam bentuk sintak program Visual Basic dan di implementasikan	Baik
5	Proses Dekripsi	• Pilih data dalam folder, tombol proses dekripsi dan tampilan kotak pesan • Algoritma MD-5 yang telah di konversi dalam bentuk sintak program Visual Basic dan di implementasikan	Baik
6	Uji Tombol Keluar	Tombol Keluar dapat di akses dengan Keyboard ataupun mouse perangkat lunak berhenti, dan pengguna keluar dari aplikasi	Baik

4. KESIMPULAN

1. Algoritma MD-5 dapat digunakan atau diterapkan pada perangkat lunak keamanan data dalam bentuk proses enkripsi dan proses dekripsi
2. Data yang di enkripsi dan dekripsi pada perangkat lunak ini adalah data yang terdapat pada Folder artinya semua data yang telah dimasukkan kedalam satu folder akan dapat di enkripsi dan dekripsikan sehingga menghemat waktu dalam proses enkripsi dan dekripsi data
3. Perangkat lunak ini hanya dapat di enkripsi dan dekripsi data dalam folder sehingga dapat dikembangkan dengan cara mengenkripsi dan dekripsi dalam bentuk file tertentu saja

DAFTAR PUSTAKA

1. Munir, Rinaldi, 2006, *Kriptografi,*. Informatika, Bandung.
2. Pressman, Rogers, 2007, *Rekayasa Perangkat Lunak,* Andi, Yogyakarta.
3. Konheim, Alan G. 2007, *Computer Security and Cryptography*, Hoboken, John Wiley & Sons. Inc, New Jersey.
4. Mollin, Richard A. 2005, *The Guide to Secrecy form ancient to Modern Times*, Boca Raton, Taylor & Francis group, LLC, New Jersey.
5. Mollin, Richard A. 2007, *An Introduction to Cryptography*, Second Edition, Boca Raton, Taylor & Francis group, LLC, New Jersey.