APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RC4

Oleh :
I GEDE AGUS BUDIAWAN
Teknik Informatika, STMIK AKAKOM Yogyakarta

ABSTRAKS

Kriptografi merupakan ilmu dan seni untuk mengamankan pesan. Kata Kriptografi (cryptography) berasal dari bahasa Yunani yaitu "cryptos" artinya "secret" (rahasia), sedangkan "graphein" artinya "writing" (tulisan). Jadi, kriptografi berarti "secret writing" (tulisan rahasia). Secara umum dikenal dua teknik dalam kriptografi yaitu Symmetric-Key (Kunci Symmetric) dan Asymmetric-Key (Kunci Asymmetric). Kunci Symmetric menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi file. Sedangkan Kunci Asymmetric menggunakan kunci yang berbeda untuk melakukan enkripsi dan dekripsi file. File yang dienkripsi dengan metode ini menggunakan public key untuk mengenkrip file dan menggunakan private key untuk mendekrip file. Karya tulis ini membahas tentang ilmu kriptografi yang kemudian akan diimplementasikannya ke sebuah bahasa pemrograman yaitu Visual Basic 6.0 untuk dijadikan sebagai sebuah tools yang berguna untuk mengamakan data. Pada Implementasi kriptografi ini, penulis menggunakan teknik Symmetric-Key atau kunci symmetric dalam proses enkripsi dan dekripsinya. Keuntungan dari enkripsi ini adalah keamanannya dan kecepatan dalam melakukan enkripsi dan dekripsi. Adapun algoritma yang digunakan dalam enkripsi ini adalah algoritma RC4, yaitu sebuah algoritma yang digunakan untuk melakukan pengacakan pesan dan password. Data yang dapat dienkripsi pada aplikasi ini hanyalah data yang berbasis biner.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, Algoritma RC4, Data Biner

PENDAHULUAN

Seiring dengan perkembangan Teknologi Informasi (Information Technology) dewasa ini, membawa dampak bagi masyarakat informasi, khususnya dibidang komputer. Komputer pada saat ini banyak sekali

digunakan pada berbagai lingkungan kegiatan. Misalnya di rumah, sekolah, kantor, industri dan lainnya. Ruang lingkupnya sudah sangat luas, sehingga sudah merambah sampai ke hal-hal yang paling kecil.

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi segolongan individu atau komunitas tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan, maka pada akhirnya orang-orang pun mengembangkan berbagai cara untuk mengatasi persoalan keamanan data agar orang-orang yang tidak berhak tidak mungkin dapat membaca atau bahkan merusak data yang bukan ditujukan kepadanya. Salah satu cara untuk melindungi data adalah dengan teknik enkripsi (encryption) yaitu sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti, sehingga data yang sudah dienkripsi tersebut tidak akan dapat dimanipulasi oleh orang yang tidak berhak untuk mengakses data tersebut. Karena teknik enkripsi merupakan suatu sistem yang telah siap untuk diautomasi, maka teknik ini digunakan untuk mengamankan data dalam disk, maupun yang sedang ditransmisikan.

METODE PENELITIAN

1. Alat dan Bahan Penelitian

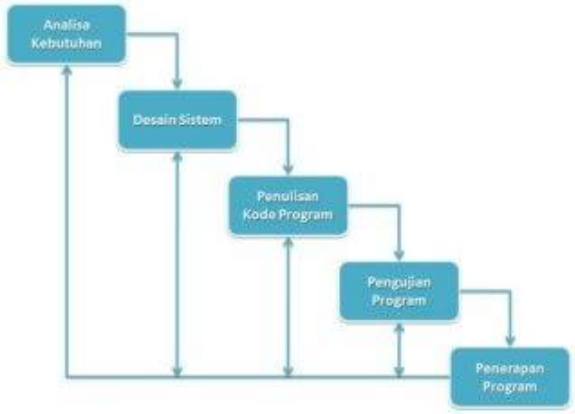
Alat dan bahan yang digunakan meliputi hardware dan software dalam penelitian ini adalah sebagai berikut :

a. Hardware
   1) Processor Intel Pentium IV 2,8 Ghz
   2) Memory RAM (random access memory) 512 mb.
   3) Keyboard dan mouse.
   4) Monitor SVGA.
   5) Harddisk dengan kapasitas 80 GB.

b. Software
   1) Sistem Operasi : Microsoft Windows XP service pack 2.
   2) Bahasa Pemrograman : Microsoft Visual Basic 6.0

2. Metode Penelitian

Untuk metode pengembangan sistem menggunakan metode waterfall menurut Pressman.



Gambar 1. Metode Waterfall

a. Analisa Kebutuhan

Langkah ini merupakan analisa terhadap kebutuhan sistem. Pengumpulan data dalam tahap ini bisa malakukan sebuah penelitian, wawancara atau study literatur. Seorang sistem analis akan menggali informasi sebanyak-banyaknya dari user sehingga akan tercipta sebuah sistem komputer yang bisa melakukan tugas-tugas yang diinginkan oleh user tersebut. Tahapan ini akan menghasilkan dokumen user requirment atau bisa dikatakan sebagai data yang berhubungan dengan keinginan user dalam pembuatan sistem. Dokumen ini lah yang akan menjadi acuan sistem analis untuk menterjemahkan ke dalam bahasa pemprogram.

b. Desain Sistem

Proses desain akan menerjemahkan syarat kebutuhan ke sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuat coding. Proses ini berfokus pada : struktur data, arsitektur perangkat lunak, representasi interface, dan detail (algoritma) prosedural. Tahapan ini akan menghasilkan dokumen yang disebut software requirment. Dokumen inilah yang akan digunakan proggrammer untuk melakukan aktivitas pembuatan sistemnya.

c. Penulisan Kode Program

Coding merupan penerjemahan design dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh programmer yang akan meterjemahkan transaksi yang diminta oleh user. Tahapan ini lah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini.

d. Pengujian Program

Setelah pengkodean selesai maka akan dilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan testing adalah menemukan kesalahan-kesalahan terhadap sistem tersebut dan kemudian bisa diperbaiki.

e. Penerapan

Tahapan ini bisa dikatakan final dalam pembuatan sebuah sistem. Setelah melakukan analisa, design dan pengkodean maka sistem yang sudah jadi akan digunakan oleh user.

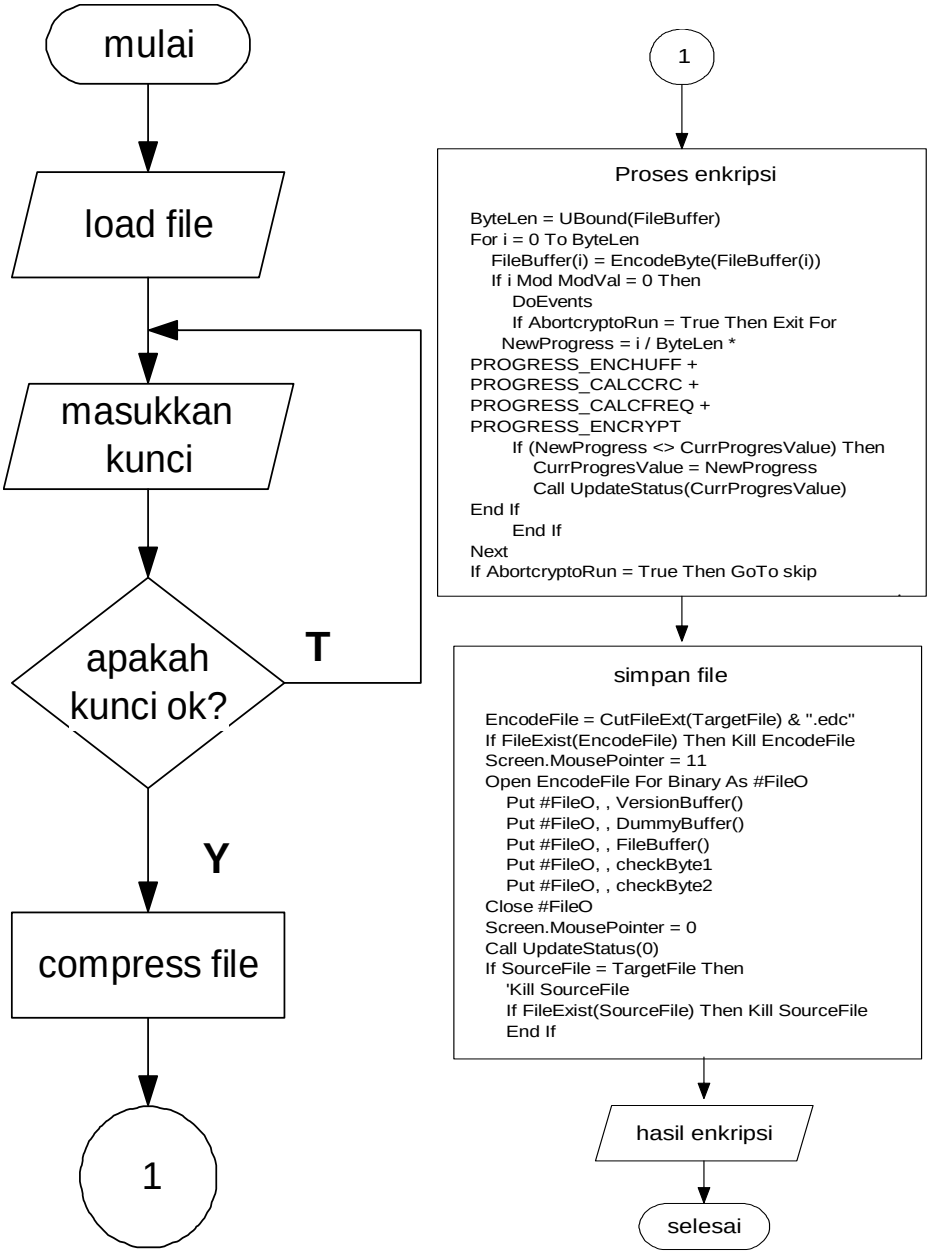
HASIL DAN PEMBAHASAN

1. Analisa Kebutuhan

Akan dibuat aplikasi enkripsi menggunakan metode enkripsi Xor, dan algoritma yang digunakan adalah algoritma RC4. Aplikasi ini hanya dapat mengolah file berbasis biner pada proses enkripsinya. Diantaranya: File Gambar (*.bmp;*.jpg;*.jpeg;*.mpeg;*gif), File Video (*.avi; *.mpg; *.mpeg; *.mp4), File Audio (*.mp3; *.midi; *.wav; *.wma) dan File Biner lain (*.doc;*.txt*.exe;*.pdf;*.rar;*.zip).

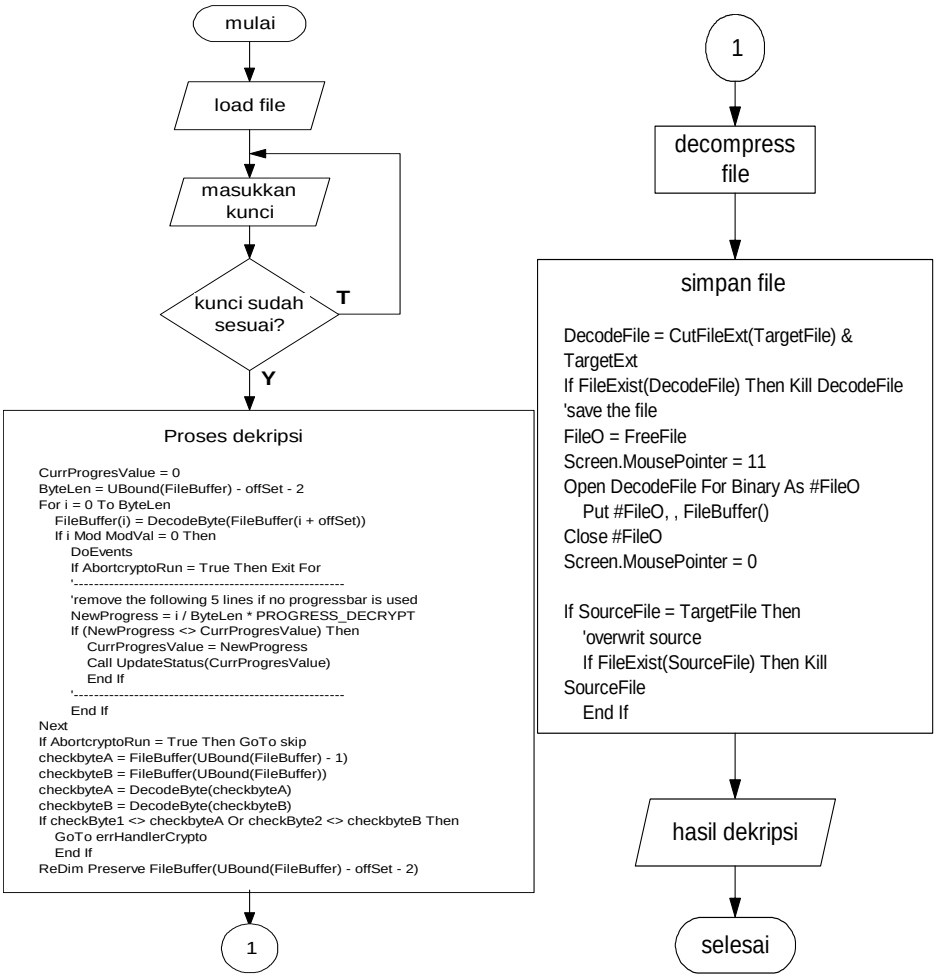
2. Desain Sistem

   a. Diagram alir proses enkripsi



Gambar 2. Diagram Alur Enkripsi

b. Diagram alir proses dekripsi



Gambar 3. Diagram Dekripsi

3. Penulisan Kode Program

Menu Kunci digunakan untuk memberikan password atau kunci pada file yang akan di enkripsi maupun di dekripsi. Berikut merupakan listing program pada menu file:

```
Private Sub mnuKey_Click()
If gstrActiveKey <> "" Then
  RetVal = MsgBox("There is already an active key." & vbCrLf &vbCrLf &"Do you want to enter a new key ?", vbYesNo + vbQuestion, "Enkripsi")
  If RetVal = vbNo Then Exit Sub
  End If
```

frmKey.Show (vbModal)

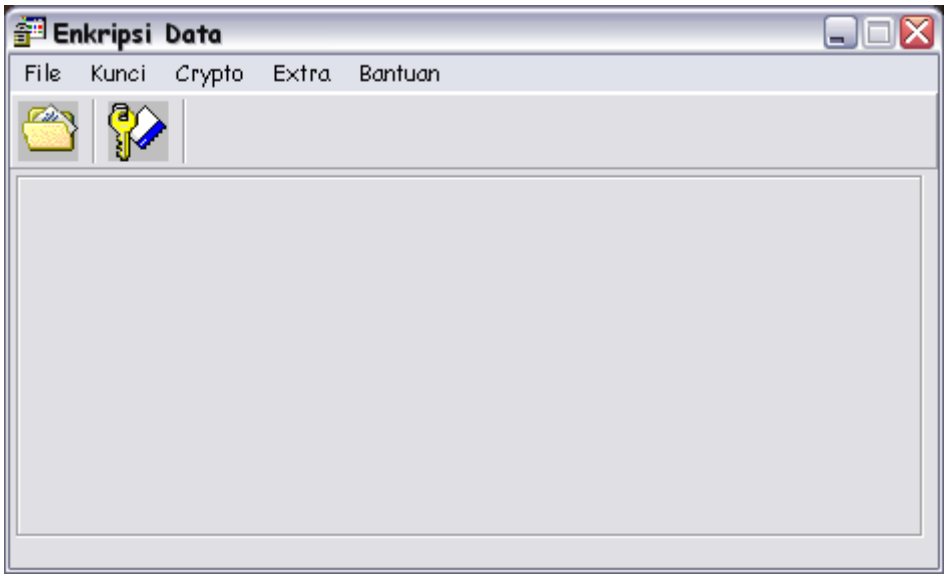
End Sub

4. Pengujian Program

Pengujian dilakukan terhadap form-form yang elah dibuat, antara lain :

a. Menu Utama

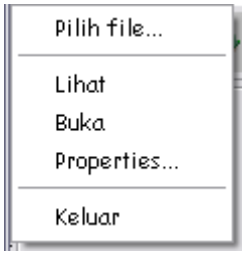
Di bawah ini adalah tampilan dari form utama yang berisi file, kunci, crypto, extra dan bantuan :



Gambar 4. Menu Utama

b. Menu File

Menu *File* merupakan menu utama untuk melakukan proses enkripsi dan dekripsi. Pada menu *file* terdapat lima sub menu yaitu: *Pilih File..*, *lihat, buka, properties* dan *keluar,* seperti terlihat pada gambar.



Gambar 5. Menu File

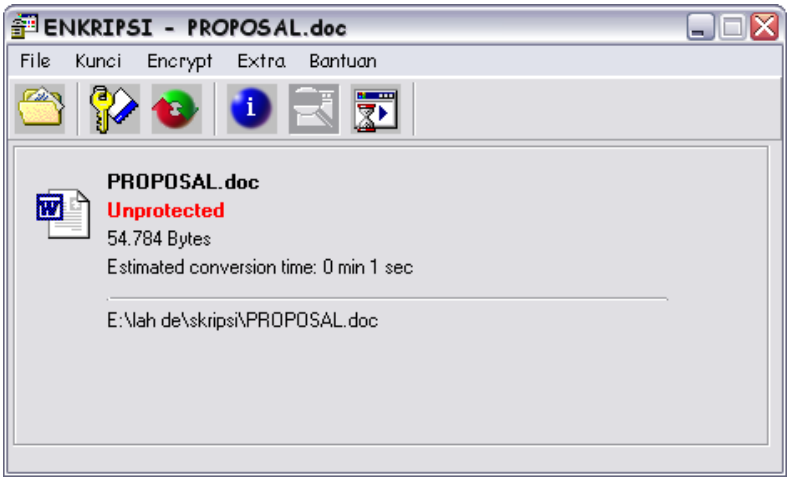
c. Menu Kunci

Menu Kunci digunakan untuk memberikan password atau kunci pada file yang akan di enkripsi maupun di dekripsi.

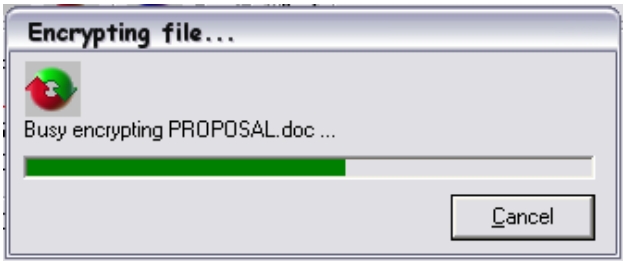
Gambar 6. Masukkan Kunci Baru

d. Menu Crypto

1) Enkripsi

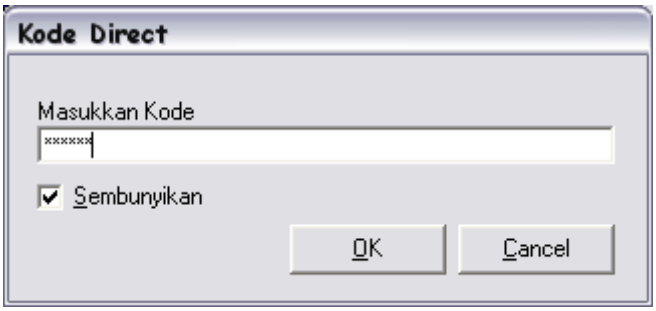


Gambar 7. Enkripsi

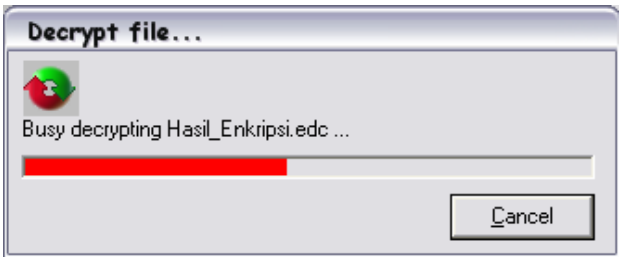


Gambar 8. Proses Enkripsi

2) Dekripsi



Gambar 9. Memasukkan Dekripsi

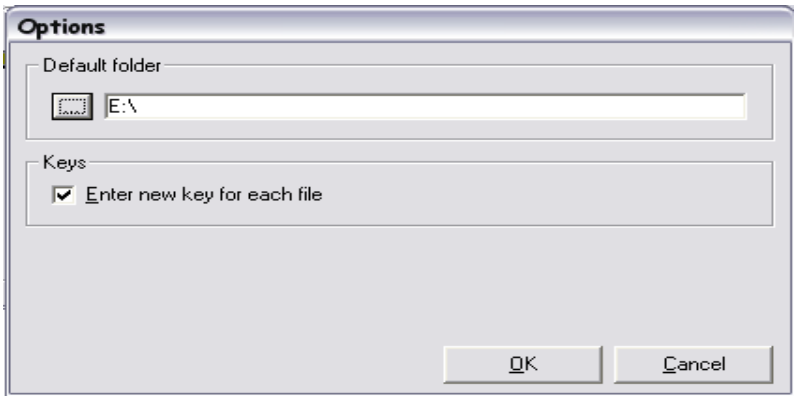


Gambar 10. Proses Dekripsi

e. Menu Extra

Menu extra merupakan menu tambahan dari aplikasi ini. Didalam menu ini terdapat submenu Options yang berfungsi untuk melakukan pengaturan default folder dan kunci.

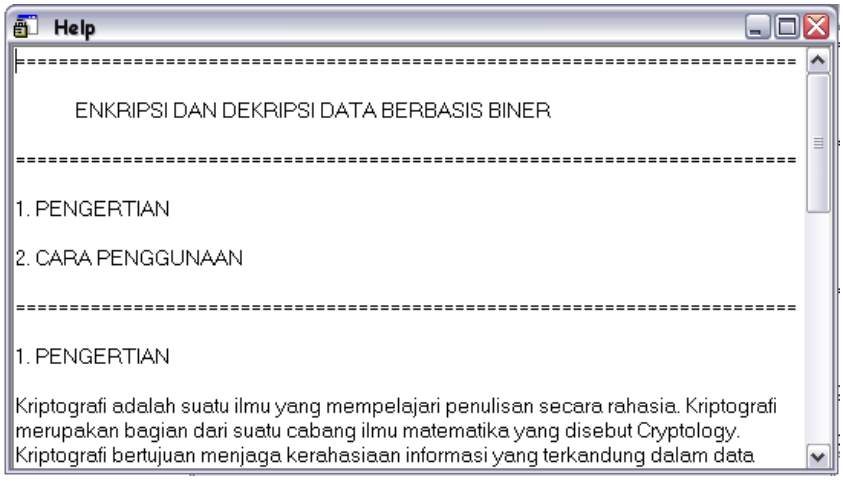
Untuk default folder, penggunakan dapat mengatur lokasi folder yang muncul saat pengguna akan mengambil file yang akan diproses. Untuk pengaturan kunci, pengguna dapat mengatur apakah akan mengganti kunci setiap pengguna mengambil file yang baru. Tampilan Form dari submenu option adalah seperti berikut:



Gambar 11. Extra

f. Menu Bantuan

Menu ini digunakan untuk menampilkan form help yang bertujuan untuk membantu pengguna menggunakan aplikasi ini. Jika submenu ini dipilih, akan menampilkan form help seperti yang terlihat pada gambar



Gambar 12. Menu Bantuan

g. Menu About

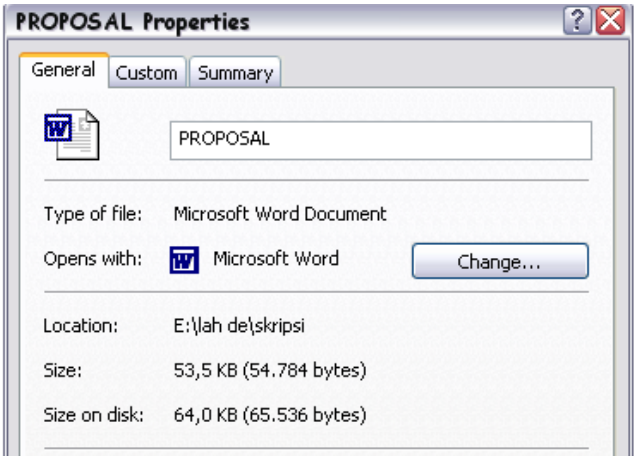
Menu ini digunakan untuk menampilkan identitas dari pembuat program dengan tampilan form seperti yang terlihat pada gambar berikut

Gambar 13. Menu About

5. Penerapan

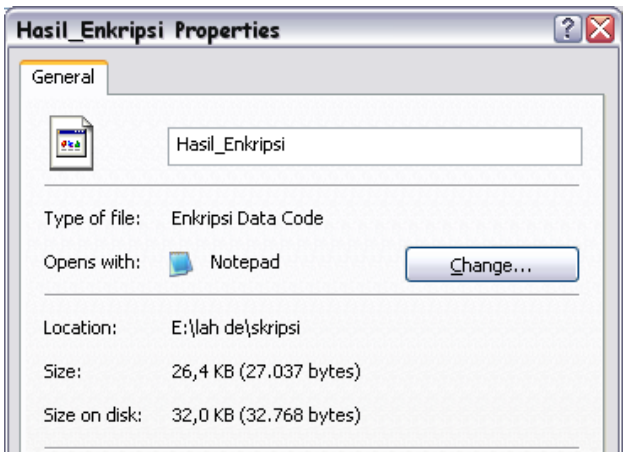
Hasil dari implementasi program ini adalah menciptakan sebuah file yang terkodekan sehingga tidak semua orang dapat mengaksesnya atau membukanya secara bebas..Untuk membuktikan seberapa aman program ini dilakukan suatu percobaan.

Percobaannya adalah dengan mengenkripsi suatu data dokumen yang dibuat menggunakan Microsoft word (*.doc). Disini akan dilakukan proses enkripsi terhadap file yang bernama "Proposal.doc".dokumen tersebut memiliki properties seperti pada gambar berikut



Gambar 14. Properties file asli

File ini akan dienkripsi dan hasilnya akan disimpan dengan nama "Hasil_Enkripsi.edc". Untuk proses enkripsinya, akan diberikan kata kunci "akakom" untuk file tersebut. Setelah dienkrip ukuran file akan berubah, hal ini di karenakan pada saat proses enkripsi terjadi proses kompresi, sehingga file hasil enkripsi akan berukuran lebih kecil dibandingkan dengan file aslinya. Gambar berikut akan memperlihatkan properties dari file hasil enkripsi



Gambar 15. Properties file hasil enkripsi

KESIMPULAN DAN SARAN

1. Kesimpulan

   Dari uraian yang telah disampaikan pada bab-bab sebelumnya mengenai Implementasi Aplikasi pengamanan data menggunakan algoritma RC4 ini, maka dapat diambil kesimpulan sebagai berikut:

   a. Perangkat lunak ini dikembangkan dengan bahasa pemrograman Visual Basic 6.0, dan hanya dapat bekerja pada sistem operasi Windows.

   b. Perangkat lunak ini dikembangkan untuk mengamankan data atau file berbasis biner.

c. Perangkat lunak ini tidak dapat mengenkripsi file hasil enkripsi, kecuali jika header file hasil enkripsi tersebut diubah terlebih dahulu.
d. Untuk mengenkripsi dan mendekripsi data yang sama, dilakukan dengan menggunakan kunci yang sama.
e. Ukuran file hasil enkripsi cenderung lebih kecil dari ukuran file asli.

2. Saran

Dalam pengembangan perangkat lunak ini selanjutnya perlu adanya perbaikan di karenakan perangkat lunak ini masih jauh dari sempurna. Adapun saran untuk lebih mendayagunakan program aplikasi ini adalah sebagai berikut:

a. Perangkat lunak ini dapat dikembangkan dan diterapkan sebagai pengaman aplikasi internet banking, layanan e-commerce, database sebuah institusi, e-mail, file transfer, dan lain sebagainya.
b. Untuk memudahkan proses pendekripsian data terenkripsi, maka perlu dibuat supaya proses dekripsi data secara otomatis berjalan ketika data terenkripsi tersebut di-double klik.
c. Untuk hasil yang lebih baik disarankan agar penelitian berikutnya menggunakan metode-metode atau algoritma steganografi dan enkripsi data yang lebih efektif dan efisien sehingga dapat meningkatkan kecepatan pengolahan data.
d. Dalam analisis pada implementasi program ini belum dibahas tentang bagaimana cara pemecahan metode dan pemecahan pesan yang telah terenkrip tanpa diketahui kata kuncinya. Untuk itu, pengembang diharapkan lebih bisa menganalisa algoritma RC4 ini yang dikhususkan pada pemecahan kata kuci yang digunakan untuk mengenkrip dan mendekrip pesan serta memecahkan pesan yang telah dienkripsi.

DAFTAR PUSTAKA

Ariyus,Dony, *"KRIPTOGRAFI Keamanan Data Dan Komunikasi"*, 2006, Graha Ilmu, Yogyakarta.

Kurniawan Tjandra. "*Tip Trik Unik Visual Basic"* , 2003, Elex Media Komputindo, Jakarta.

Pamungkas, Ir, "*Tip & Trik Microsoft Visual Basic 6.0*", 2000, Elex Media Komputindo, Jakarta.

Pramono, Djoko, "*Mudah Menguasai Visual Basic 6.0*", 1999, Elex Media Komputindo, Jakarta.

Ramadan Arief, "*Seri Penuntun Praktis Microsoft Visual basic 6"*. 2004, Elex media Komputindo, Jakarta.

Wahana komputer semarang, "*Memahami Model Enkripsi & Security Data*", 2003, Penerbit ANDI, Yogyakarta.

Wahana Komputer Semarang & Andi Offset. "*TIP & TRIK Pemrograman Visual Basic 6.0" ,* 2001, Andi Offset, Yogyakarta.