

Perancangan Aplikasi Folder Lock Dengan Metode DES

Christopel Daniel¹⁾ Willy Putradi Angkasa²⁾

STMIK IBBI Medan

Jl. Sei Deli No. 18 Medan, Telp. 061-4567111 Fax. 061-4527548

Email: Christopherdanil@gmail.com

Abstrak

Pada saat ini, telah banyak aplikasi yang diciptakan untuk membantu kemudahan dalam penggunaan komputer. Salah satu aplikasi yang paling sering dicari adalah aplikasi yang dapat membantu meningkatkan keamanan pada komputer, sehingga data atau informasi yang bersifat pribadi maupun rahasia tidak akan dapat diakses secara sembarangan oleh orang yang tidak berkepentingan. Aplikasi ini terutama paling sering dicari oleh perusahaan atau organisasi, dikarenakan banyaknya data atau informasi yang dimiliki oleh perusahaan atau organisasi yang tidak boleh diketahui oleh semua orang. Aplikasi Folder Lock ini dirancang dengan menggunakan metode DES yang telah terbukti cukup tinggi tingkat keamanannya. Mengingat suatu data atau informasi biasanya disimpan pada sebuah folder atau direktori, maka hasil dari aplikasi yang dirancang ditujukan untuk meningkatkan keamanan pada folder atau direktori.

Kata Kunci : Folder, Direktori, Aplikasi, Keamanan, DES.

Abstract

At this time, many applications have been created to help ease the use of computers. One of the most frequently sought are applications that can help improve security on the computer, so that the data or information that is private and confidential will not be accessible from random people who are not interested. The application is mainly the most frequently sought by the company or organization, because many of the data or information held by the company or organization that should not be known by everyone. Folder Lock application is designed using DES method which has proven to be quite a high level of security. Given the data or information is usually stored in a folder or directory, then the result of the intended application designed to improve security at the folder or directory.

Keywords: Folder, Directory, Application, Security, DES.

1. Pendahuluan

Perkembangan teknologi informasi dewasa ini yang demikian pesat dengan hadirnya komputer dalam kehidupan manusia mulai dari tahun 1940 sampai sekarang telah mengalami berbagai perkembangan, mulai dari kemampuan *hardware* maupun kemampuan *software* yang terus berkembang. Di dalam perkembangan *software* terutama sistem operasi yang digunakan sekarang ini telah mengalami beberapa fase perkembangan mulai dari *Disk Operating System* (DOS), *Linux*, *OS/2*, *Windows* maupun yang lainnya. Sedangkan untuk sistem operasi *Windows* sendiri juga telah mengalami beberapa fase perkembangan yang dimulai dari *Windows* versi 1.0, *Windows* 3.0, 3.1 sampai *Windows* XP, NT dan sekarang *Windows* 7.

Keamanan informasi dewasa ini dirasakan sangat penting. Hal ini bisa dipahami karena informasi merupakan hal yang sangat dibutuhkan oleh organisasi atau perusahaan, maupun untuk pribadi. Dalam sebuah organisasi atau perusahaan tentunya terdapat data atau informasi yang rahasia yang tidak boleh diakses oleh pihak yang tidak berkepentingan. Oleh karena itu, pengamanan dalam sebuah organisasi atau perusahaan perlu terus diperhatikan agar tidak terjadi pencurian data atau informasi oleh pihak luar yang tidak berkepentingan atau terjadinya kerusakan data yang disebabkan oleh virus. Terutama jika data atau informasi tersebut berada pada suatu sistem komputer, jaringan komputer bahkan dalam jaringan internasional yang sering disebut internet.

Disebabkan luasnya permasalahan yang ada, maka peneliti memberikan batasan masalah antara lain:

1. Aplikasi yang dibuat dibatasi agar *compatible* pada *Operating System* *Windows* XP.
2. Hard Disk yang digunakan telah menggunakan *file system* NTFS.
3. Perancangan program menggunakan bahasa pemrograman *Microsoft Visual Basic 6.0*.

2. Metode Penelitian

Sebuah *directory*(Folder) adalah seperti ruangan-ruangan(kamar-kamar) pada sebuah komputer yang berfungsi sebagai tempat penyimpanan dari berkas-berkas (File). Sedangkan File adalah kumpulan data-data baik berupa teks, angka, gambar, video, slide, program, dan lain-lain yang diberi nama tertentu secara digital.

Folder Lock adalah sebuah *software* yang dapat mengunci *Folder*(*Directory*) beserta dengan *file* di dalamnya sehingga tidak dapat diakses oleh sembarang orang. Jika ada yang hendak mengakses *Folder* yang

dikunci tersebut, maka *user* harus membuka *folder* tersebut terlebih dahulu dengan memasukkan *Password* yang telah dimasukkan sebelumnya.

Bagi orang yang sering menggunakan komputer, tentunya telah mengetahui bahwa *Folder(Directory)* memiliki *attribute*. *Attribute* itu dapat kita lihat dengan cara klik kanan pada salah satu *Folder* kemudian pilih *properties*, maka akan terlihat *attribute Folder Read-Only, Archive, & Hidden*. Namun, tidak semua orang tahu *Windows* memiliki *attribute-attribute* lain yang tidak ditampilkan. Salah satunya adalah *attribute System* (kadang disebut juga sebagai *SuperHidden*) yang biasa digunakan *Windows* untuk menyembunyikan komponen-komponen *Folder* penting bagi *Windows*. Pada pembuatan *Folder Lock* ini, *attribute System* juga akan diberikan pada *Folder* yang dipilih, sehingga *Folder* tidak akan tampak walaupun tanda “*Show Hidden Folder*” telah diberikan pada *Folder Option*. Dalam memberikan *attribute System* pada *Folder*, *Function* yang akan digunakan adalah *Function* yang biasa diakses melalui *cmd*. *Function* tersebut adalah *Function* “*attrib*” yang menggunakan *Attrib.exe* yang berada pada *Folder %windir%/system32*.

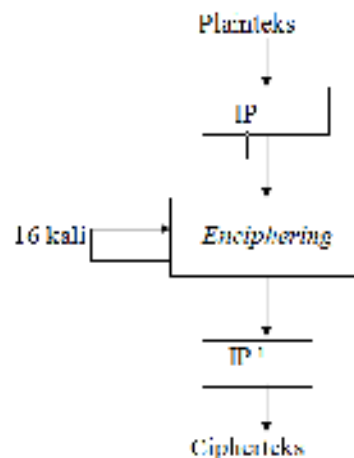
Di dalam *Windows* sebenarnya terdapat suatu fungsi yang dapat digunakan untuk mengunci *folder* pribadi, sehingga tidak dapat diakses oleh orang yang tidak berkepentingan. Fungsi tersebut adalah dengan mengubah *access permission* dari *folder* tersebut. Sayangnya, fungsi ini hanya sedikit yang mengetahui dan hanya dapat berjalan pada *HardDisk* yang telah menggunakan sistem *NTFS*. *Access Permission* ini juga baru diaplikasikan mulai dari *Windows XP*. Cara kerja dari *access permission* ini mirip dengan *access permission* yang diberikan sewaktu pengguna *login* dengan *Id* yang berbeda pada sebuah komputer yang mempunyai sistem operasi *Windows*. Jika pengguna membuka *Windows* dengan suatu *Id*, maka pengguna tersebut tidak dapat mengakses *folder* milik *Id* lain.

Perintah yang digunakan untuk menjalankan fungsi ini adalah *CACLS.exe* yang secara *default* telah ada pada *Windows XP* yang biasanya terletak pada “*C:\windows\system32*”(dengan anggapan *Windows* diletakkan pada *Drive C*). Program *CACLS* ini merupakan singkatan dari *Change Access Control List* yang berfungsi untuk mengubah *ACLs* pada *Windows*. Secara sederhana, *ACLs* adalah sebuah daftar yang menjelaskan pengguna mana yang dapat mengakses suatu *folder* atau data tertentu. Yang artinya, pengguna bisa saja tidak memberikan *access* kepada orang lain(baca:*account* lain) terhadap milik pengguna tersebut ataupun sebaliknya. *CACLS* juga dapat digunakan walaupun pada komputer tersebut hanya memiliki satu *account* saja yang tidak perlu melalui *login Windows*. Hal ini dapat dilakukan dengan tidak memberikan *access permission* pada *account* itu sendiri, sehingga data atau *folder* tersebut tidak dapat diakses oleh siapapun pada komputer tersebut. *CACLS* dapat diakses dengan menggunakan *command prompt*. Untuk perintah lengkap dari *CACLS* juga dapat dilihat pada *command prompt* itu sendiri.

2.1. Model

Secara umum, algoritma *DES* terbagi menjadi 3 kelompok dimana kelompok yang satu dengan yang lain saling berinteraksi dan terkait antara satu dengan yang lain. Kelompok-kelompok tersebut adalah pemrosesan kunci, enkripsi data 64-bit, dan dekripsi data-64 bit.

Algoritma *DES* dirancang untuk menulis dan membaca berita blok data yang terdiri dari 64 bit dibawah control kunci 64-bit. Dalam pembacaan berita harus dikerjakan dengan menggunakan kunci yang sama dengan waktu menulis berita, dengan penjadwalan alamat kunci bit yang diubah sehingga proses membaca adalah kebalikan dari proses menulis. Sebuah blok ditulis dan ditujukan pada permutasi dengan inisial *IP*, kemudian melewati perhitungan dan perhitungan tersebut sangat tergantung pada kunci kompleks dan pada akhirnya melewati permutasi yang invers dari permutasi dengan inisial IP^{-1} . (Wahana Komputer Semarang : hal 186-187)



Gambar 1. Skema Global Algoritma DES

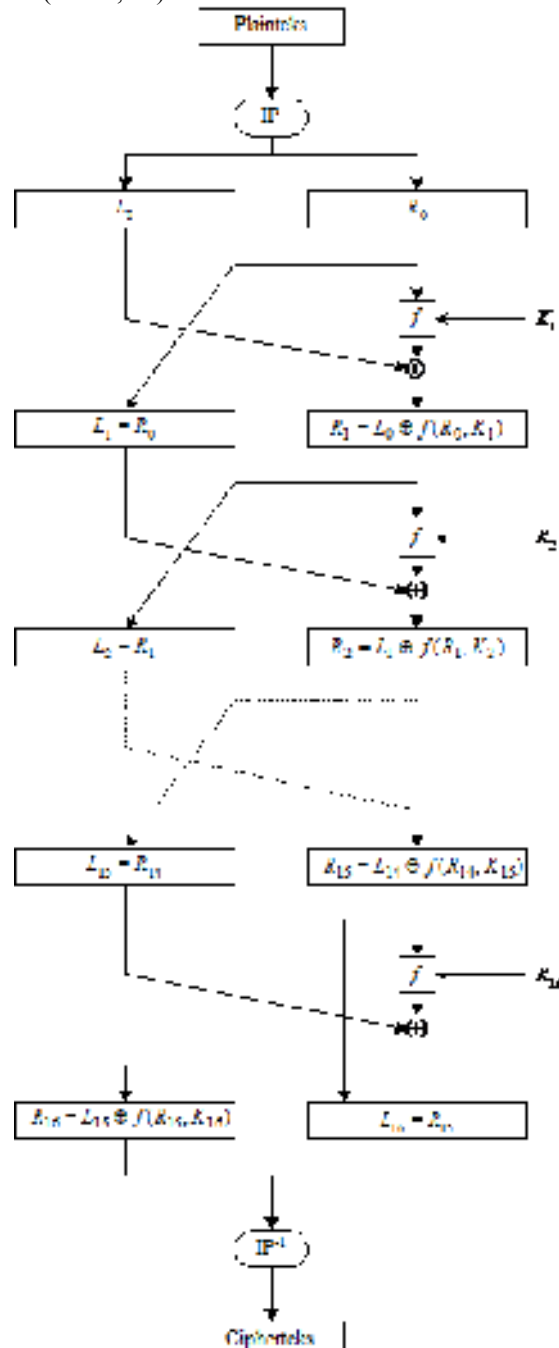
Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES.

Pada setiap putaran i , blok R merupakan masukan untuk fungsi transformasi yang disebut f . Pada fungsi f , blok R dikombinasikan dengan kunci internal K_i . Keluaran dari fungsi f di-XOR-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelumnya. Ini adalah satu putaran DES.

Secara matematis, satu putaran DES dinyatakan sebagai

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$



Gambar 2. Algoritma Enkripsi dengan DES

2.2. Analisis dan Desain

Untuk rancangan *Flowchart* dari perangkat lunak *Folder Lock* dapat dilihat pada Gambar 3.

3. Tampilan *Form Main Menu*

Tampilan *form Main Menu* merupakan tampilan utama dari perangkat lunak yang berfungsi sebagai tempat penambahan *folder* yang ingin dikunci oleh pengguna, serta sebagai tempat untuk *unlock folder*, *delete folder*, dan penjelasan cara penggunaan perangkat lunak *Folder Lock*. Tampilan *form 'Main Menu'* dapat dilihat pada gambar 6 berikut:



Gambar 6. Tampilan *Form Main Menu*

4. Tampilan *Form Change Password*

Tampilan *form Change Password* merupakan tampilan dari perangkat lunak yang berfungsi sebagai tempat untuk mengganti *Master Password* dari perangkat lunak. Tampilan *form 'Change Password'* dapat dilihat pada gambar 7 berikut:



Gambar 7. Tampilan *Form Change Password*

3. Hasil dan Pembahasan

Perbandingan program ini dilakukan dengan membandingkan aplikasi Folder Lock yang dirancang dengan aplikasi Folder Lock 6.6 yang sering dipakai oleh pengguna komputer dalam mengunci *folder*. Adapun hasil perbandingan antara aplikasi Folder Lock yang dirancang dengan aplikasi Folder Lock 6.6 dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan Aplikasi Folder Lock yang Dirancang dengan Folder Lock 6.6

Perbandingan	Folder Lock yang dikembangkan	Folder Lock OS
OS	Windows XP/Windows 7	Windows 2000/ME/9x/2003/XP/Windows 7
Tampilan	Tidak membingungkan	Dapat membingungkan pengguna baru
Spesifikasi	Cepat	Sebelumnya
Akses folder	Mudah	Sebelumnya
Melakukan folder	Sedikit ada di hardisk, Evolusi	Tidak ada jika di hardisk
Keamanan	NTFS	Kompartemen dengan akses Administrator
Kelebihan	Lebih sederhana	Lebih & Lebih
Kelemahan	Tidak ada	Lebih & Lebih

4. Kesimpulan dan Saran

4.1. Kesimpulan

Berdasarkan hasil penelitian, disimpulkan sebagai berikut.

1. Folder(*directory*) dapat dikunci sehingga tidak dapat diakses tanpa memasukkan *password* pada aplikasi yang telah dibuat terlebih dahulu.
2. Dari pengujian program terlihat bahwa tampilan aplikasi cukup *user friendly*, sehingga dapat digunakan dengan mudah bahkan oleh pengguna yang baru menggunakan aplikasi.
3. Kesimpulan akhir dari penelitian ini adalah aplikasi *Folder Lock* yang telah dibuat dapat berfungsi untuk mengunci folder(*directory*) sebagaimana mestinya tanpa membingungkan pengguna perangkat lunak.

4.2. Saran

Adapun saran untuk pemakaian dan pengembangan perangkat lunak ini adalah sebagai berikut:

1. Menambahkan tingkat keamanan dari aplikasi folder lock dalam bentuk kombinasi dengan algoritma kriptografi selain DES
2. Memastikan bahwa aplikasi dapat digunakan untuk harddisk selain NTFS
3. Dapat dipergunakan untuk multi user,

Daftar Pustaka

- [1] Wahana Komputer Semarang, 2003, *Memahami model enkripsi & security data*, Penerbit Andi, Yogyakarta.
- [2] Wahana Komputer Semarang, 2003, *Pemrograman Visual Basic 6.0*, Penerbit Andi, Yogyakarta.
- [3] Anonim, 2011, *Attrib.exe*, <http://ss64.com/nt/attrib.html>. Diakses pada tanggal 21 Agustus 2011.
- [4] chamim18, 2010, *Folder Lock (maksudnya ngunci folder) ala Windows* <http://chamim18.wordpress.com/2010/05/27/folder-lock-maksudnya-ngunci-folder-ala-windows-2/>. Diakses pada tanggal 20 Agustus 2011.
- [5] Nanpunya, 2009, *Mengenal File dan Folder*, <http://nanpunya.wordpress.com/2009/03/11/mengenal-file-dan-folder>. Diakses pada tanggal 20 Agustus 2011.
- [6] Recinay, 2010, *Pengertian Windows XP*, recinay.wordpress.com/2010/04/03/windows-xp. Diakses pada tanggal 20 Agustus 2011.
- [7] Rifandi02, 2010, *Cara membuat Folder Lock melalui Notepad*, <http://rifandi02.wordpress.com/2009/11/13/cara-membuat-folder-lock-melalui-notepad/>. Diakses pada tanggal 21 Agustus 2011.