PENGEMBANGAN APLIKASI KRIPTOGRAFI FILE DOKUMEN, AUDIO DAN GAMBAR DENGAN ALGORITMA DES

Irmawati

Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional
Email: irmawati@civitas.unas.ac.id

ABSTRAK

Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi sangatlah penting. Seringkali data atau informasi yang penting dalam komunikasi dan pertukaran informasi kadang tidak sampai kepada penerima atau tidak hanya diterima oleh penerima tetapi juga oleh pihak lain yang melakukan pembajakan atau penyadapan. Untuk mengatasi masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simetris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma yang digunakan adalah DES (Data Encryption Standard). Aplikasi yang dibuat mampu mengenkripsi file dokumen, video, gambar dan audio.

Kata Kunci: Kriptografi, Simetris, Algoritma DES

1. PENDAHULUAN

1.1 Latar Belakang

Kemajuan sisi teknologi komputer dan telekomunikasi bagaikan pisau bermata dua. Disatu sisi kita dimudahkan dengan adanya teknologi itu, namun disisi lain aspek kejahatan dengan menggunakan teknologi ini juga semakin meningkat, maka dari itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas tertentu. Aplikasi keamanan data pada dasarnya memiliki tiga faktor yang perlu dipertimbangkan, yaitu tingkat kesulitan untuk meng-crack atau menembus pesan yang dienkrip menggunakan suatu metode enkripsi, kecepatan dalam melakukan enkripsi dan dekripsi, dan keamanan dari kunci. Selain itu faktor yang tidak kalah penting adalah jenis data yang bisa di enkripsi dan dekripsi. Aplikasi pembanding yang menjadi acuan pada penulisan ini rata-rata memiliki keamanan kunci yang lemah karena panjang bit yang dihasilkan masih rendah, selain itu tidak semua jenis file bisa di enkripsi. Berdasarkan uraian diatas, maka akan dibuat suatu aplikasi keamanan data yang memiliki keamanan kunci yang kuat, kecepatan enkripsi dan dekripsi yang tinggi, dan mampu mengenkripsi file dokumen,audio,video dan gambar dengan menggunakan teknik enkripsi DES (*Data Encryption Standart*).

2. TUJUAN

Mengembangkan aplikasi keamanan data dengan menyempurnakan kekuatan kunci enkripsi pada file dokumen,video, gambar dan audio.

3. MANFAAT PENELITIAN

Manfaat terapan hasil penelitian; sebagai aplikasi keamanan data dengan kekuatan kunci enkripsi yang dapat digunakan pada pengamanan file dalam bentuk dokumen,video,gambar dan audio.

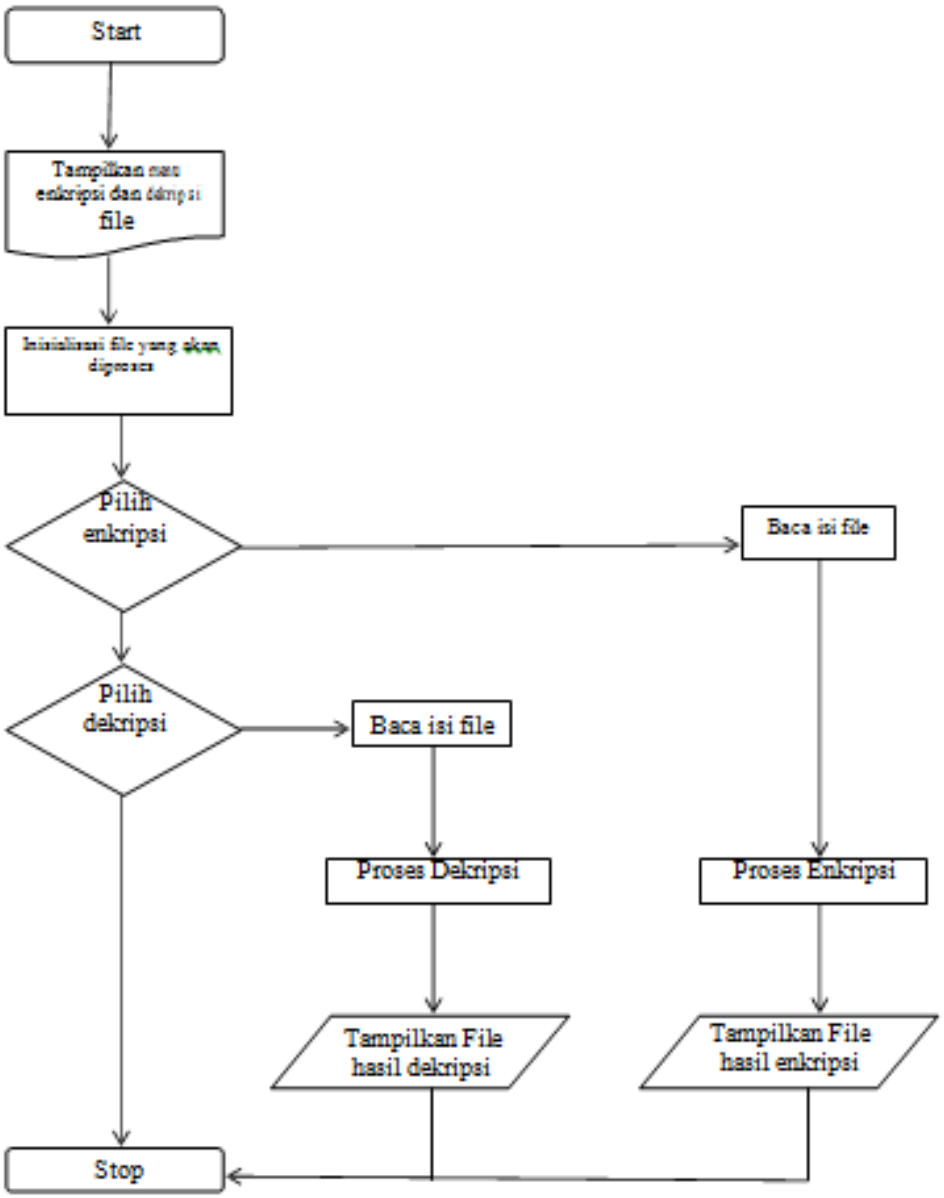
4. METODE PENELITIAN

Pada penelitian ini untuk proses penyusunan laporan sampai pembuatan aplikasi dibutuhkan data-data yang menunjang proses penelitian terutama data yang berhubungan dengan teknik kriptografi dengan algoritma DES. Dalam mengumpulkan data yang diperlukan untuk melakukan penelitian ini, digunakan beberapa metode yaitu:

1) Metode Observasi
   Pada pembuatan aplikasi kriptografi ini metode observasi diterapkan pada pembuatan laporan dan program, misalnya dengan meneliti file audio,dokumen dan gambar dengan format apa saja yang bisa digunakan pada proses kriptografi dengan algoritma DES.
2) Metode studi kepustakaan *(Literature Study)*
   Merupakan metode dengan menggunakan referensi-referensi yang ada hubungannya dengan masalah yang dijadikan objek penelitian.

Metode yang digunakan untuk menganalisa data dalam penelitian ini adalah dengan melakukan wawancara langsung dengan beberapa responden yang menguasai materi-materi yang dijadikan objek penelitian. Serta mencari dan mempelajari literatur-literatur yang berkaitan dengan pengamanan informasi pada jaringan internet umumnya dan kriptografi pada khususnya.

Adapun proses sistem secara garis besar dapat digambarkan dengan konteks diagram alir program berikut ini:

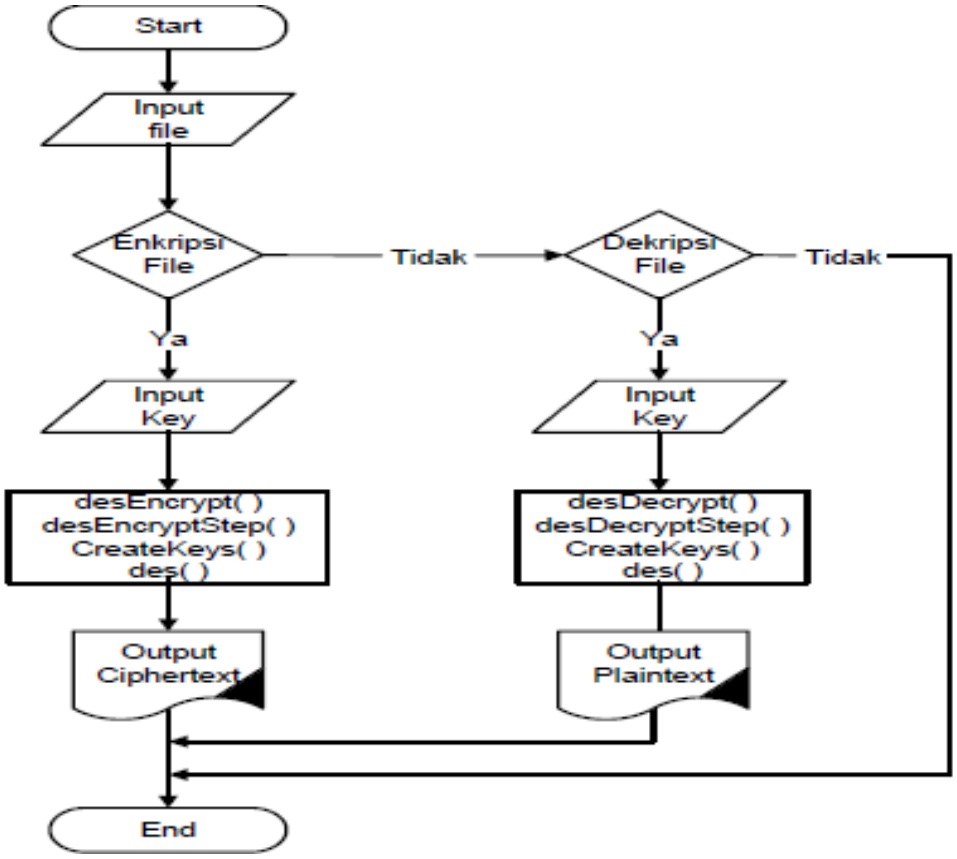


Gambar 1 Diagram Alir Aplikasi

5. KAJIAN PUSTAKA

Beberapa penelitian yang pernah dilakukan sebelumnya berkenaan dengan sistem pengamanan data menggunakan Algoritma DES *(Data Encryption Standartd).*

Penelitian yang dilakukan oleh I Putu Heryawan, 2011 yang membuat sebuah aplikasi untuk pengamanan data pada file – file yang dianggap penting yang disimpan pada komputer dengan menggunakan algoritma DES dengan melakukan pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit. Kelemahan dari aplikasi ini yaitu sistem penyandiaan data yang masih menggunakan enkripsi data 64 bit, sehingga harus dikembangkan lagi dengan enkripsi data 128 bit, dan dekripsi data 128 bit.



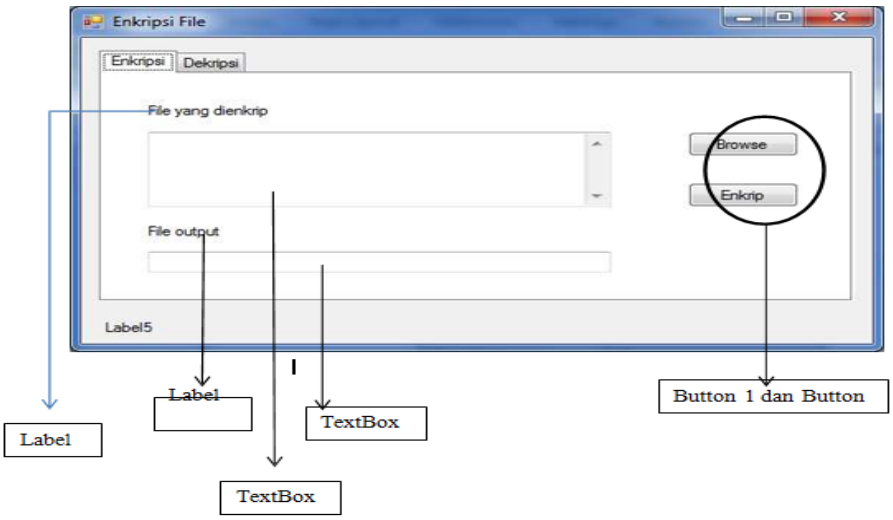
Gambar 2 Flowchart Proses Enkripsi dan Dekripsi Pada Metode DES

Penelitian oleh Yoga bagus Perkhasa, Wahyu Suadi, Baskoro Adi Pratomo, 2012,dimana penelitian ini menerapkan steganografi dengan teknik Parity Coding pada media audio wav dengan implementasi steganografi disertai dengan penerapan kriptografi berupa enkripsi dan dekripsi. Teknik Kriptografi yang digunakan adalah DES.

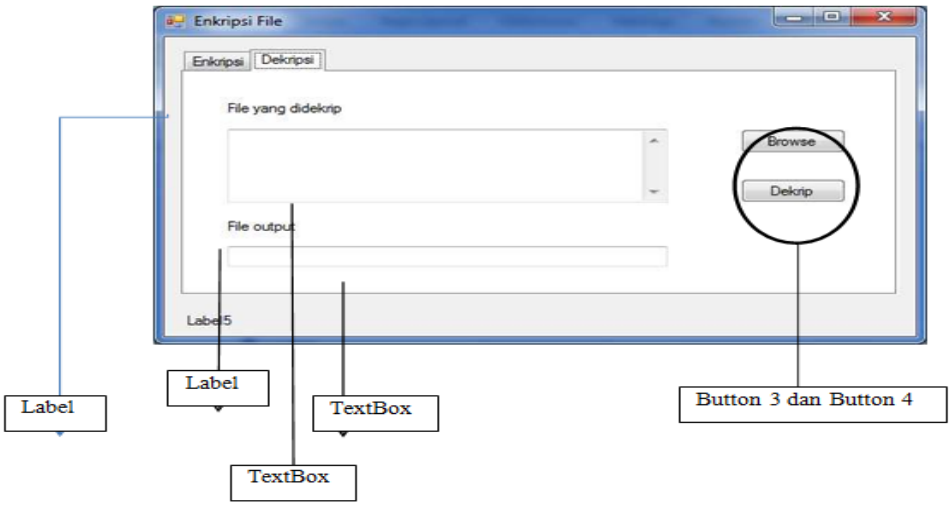
6. PEMBAHASAN

6.1 Implementasi

Pembangunan antarmuka pada tulisan ini dibangun dengan pemrograman Visual Basic .Net 2008. Berikut ini adalah tabel objek-objek yang diimplementasikan di masing-masing aktifitas program.



Gambar 3 Aktifitas Tab Enkripsi

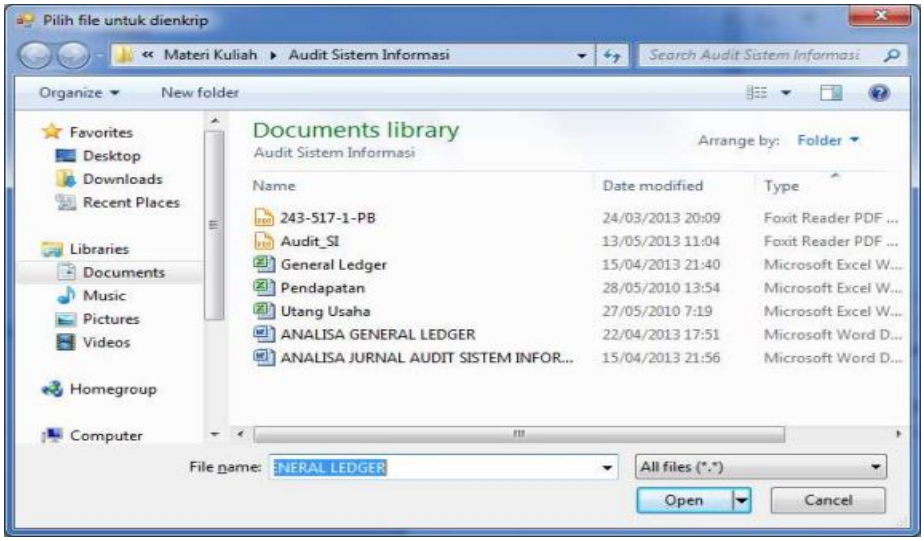


Gambar 4 Aktifitas Tab Dekripsi

Pada aplikasi ini proses enkripsi dan dekripsi tidak dipisahkan halamannya, melainkan dipisahkan oleh komponen TabControl. Pada halaman diatas terdapat beberapa tombol yang berfungsi:

1) Button 1

Tombol ini merupakan tombol Browse pada tab Enkripsi yang berfungsi untuk mencari file yang ingin di enkripsi. Jika tombol tersebut diklik maka akan muncul tampilan seperti dibawah ini.



Gambar 5 Form Pencarian File

Gambar 6 Form Input Password

Gambar 6. merupakan form input password, password yang bisa dimasukkan minimal 8 karakter. Setiap file memiliki passwordnya masing-masing, jadi setiap file yang terenkipsi passwordnya berbeda-beda. Pilih OK untuk enkripsi.

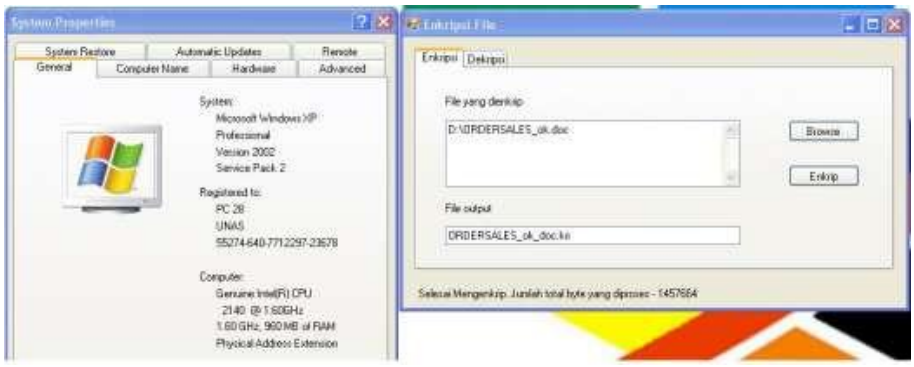
7. PENGUJIAN

Dalam tahap ini akan dilakukan pengujian aplikasi. Pengujian aplikasi terdiri dari pengujian platform aplikasi, pengujian blackbox, kekuatan kunci enkripsi, serta kecepatan enkripsi file.

7.1 Pengujian Platform Aplikasi

Pengujian platform aplikasi adalah melakukan pengujian aplikasi terhadap beberapa platform windows dengan versi yang berbeda-beda mulai dari Windows XP sampai Windows 7.

1) Pengujian Pada Windows XP 32-bit
   Berikut ini adalah pengujian yang dilakukan pada Windows XP 32-bit.



Gambar 7 Pengujian Pada Windows XP 32-bit

Gambar diatas menunjukkan bahwa pada Windows XP 32-bit aplikasi berjalan lancar. Begitu pula dengan proses enkripsi dan dekripsinya. Pada windows versi ini aplikasi kompatibel untuk dijalankan.

7.2 Pengujian Kekuatan Kunci Enkripsi

Pengujian ini dilakukan untuk mengetahui apakah file yang sudah terenkripsi dapat dengan mudah dilakukan dekripsi. Menurut Institusi Electronic Frontfier Foundation secara teoritis semua algoritma enkripsi dapat dipecahkan, tetapi sebuah algoritma enkripsi dikatakan aman jika waktu untuk memecahkannya dibutuhkan waktu lama. Pengujian akan dilakukan dua tahap yaitu manipulasi ekstensi file, dan menggunakan software File Repair. Jenis file yang diuji juga dibagi menjadi tiga golongan yaitu dokumen (docx, pptx, xllsx, pdf), media (mp3, mkv, avi, jpg, png), dan utilitas (rar, exe).

7.3 Pengujian Menggunakan Software File Repair

File Repair merupakan software untuk memperbaiki file yang sudah rusak dan tidak bisa dibuka kembali. Penggunaan software ini dikarenakan file yang sudah terenkripsi dengan aplikasi keamanan data akan terbaca corrupt.

7.4 Pengujian Kecepatan Enkripsi

Menurut Institusi Electronic Frontfier Foundation algoritma kriptografi harus bisa menangani file-file besar dalam waktu cepat. Pengujian ini dilakukan terhadap spesifikasi komputer seperti processor dan RAM serta ukuran dari sebuah file.

8. KESIMPULAN

Kesimpulan yang didapat dari penelitian ini adalah sebagai berikut:

1) Aplikasi ini dapat mengenkripsi seluruh jenis ekstensi dari sebuah file.
2) Kekuatan kunci enkripsi Data Encryption Standard lebih baik dibandingkan dengan MD5 dan RC4, hal ini dibuktikan dengan hasil pengujian dengan manipulasi ekstensi file dan penggunaan software pembuka enkripsi yaitu file repair.
3) Kecepatan enkripsinya yaitu 5549,9 KiloByte/Detik atau 5,41 MegaByte/Detik.
4) *Data Encryption Standard* merupakan algoritma kriptografi simetris karena hanya menghasilkan satu kunci private dengan ukuran 56 bit.

DAFTAR PUSTAKA

[1] Cheriandika. A, Putu. 2004. *Aplikasi penyisipan data dengan menggunakan teknik steganografi pada file Audio WAV*.
[2] Herryawan, I Putu. 2011. *Analisa dan Penerapan Algoritma DES unuk Pengamanan Data Gambar dan Video*. Universitas Udayana.
[3] Kadir, Abdul. 2002. *Apa & Bagaimana E-Commerce, Edisi Pertama, Cetakan ke-2*. Yogyakarta: Penerbit Wahana Komputer dan Andi Offset. Ir. Yusuf Kurniawan.MT , KRIPTOGRAFI Keamanan Internet dan Jaringan Komunikasi, penerbit Informatika Bandung, 2004
[4] Perkhasa, Yoga Bagus., dkk. 2012. *Implementasi Kriptografi dan Steganografi pada File Audio Menggunakan Metode DES dan Parity Coding*. ITS- Surabaya: Informatika ITS.
[5] Rahardjo, B. 2003. *Memahami Model Enkripsi & Security Data*. Yogyakarta: Penerbit Wahana Komputer dan Andi Offset.