Majapahit Techno, Agustus 2017, Hal. 33-40
ISSN : 2087-9210

Vol. 6 No. 2

RANCANG BANGUN APLIKASI KRIPTOGRAFI DENGAN METODE ENKRIPSI FILE MENGGUNAKAN GABUNGAN ALGORITMA DES DAN CAESAR CHIPER UNTUK KEAMANAN DOKUMEN

(Design Of Cryptography Applications With Encryption File Method Uses a Combination Of Des Algorithms And Caesar Cipher Algorithms For Document Security)

Khoirun Nisa, Mimin F Rohmah, Sugianto
Program StudiTeknik Informatika, Universitas Islam Majapahit
Email: riyan.asr80@gmail.com; miminfr@gmail.com

ABSTRAC

Security and confidentiality when exchanging data and information become important in the era of information and communication technology today. One of the security techniques that can be learned and developed is cryptography. Along with the development of technology, the method used is also growing, such as the use of computer as a means of storing and transmitting data, information, and confidential documents are important and can often be easily accessed by people who are not responsible. Security and confidentiality of data on computer networks today become a very important issue and continues to grow. In this thesis create applications by combining methods Cryptography Application with File Encryption Method using Combined Algorithm Des and Caesar ChiperFor Document Security will generate data more secure. In the test results of the resulting application, the application can encrypt all file documents, audio, video and image. And the results obtained on the determinants of success or failure of the encryption was not dependent on the format of the file but the file size, file sizes can all except GB. namely the large file size with the size of 2.32 GB.

Keywords: *Cryptography, DES, Caesar Cipher, File Documents.*

ABSTRAK

Keamanan dan kerahasiaan saat melakukan pertukaran data dan informasi menjadi hal yang penting pada era teknologi informasi dan komunikasi saat ini. Salah satu teknik pengamanan yang bisa dipelajari dan dikembangkan adalah kriptografi. Seiring dengan perkembangan teknologi, metode yang digunakan juga terus berkembang, seperti penggunaan Komputer sebagai sarana penyimpanan dan pengiriman data, informasi, dan dokumen yang penting dan rahasia sering dapat dengan mudah diakses oleh orang yang tidak bertanggung jawab. Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Pada tugas akhir ini membuat aplikasi dengan menggabungkan metode Aplikasi Kriptografi dengan MetodeEnkripsiFilemenggunakan Gabungan Algoritma Des Dan Caesar Chiper Untuk Keamanan Dokumen yang akan menghasilkan data yang lebih aman. Pada hasil uji coba dari aplikasi yang dihasilkan, aplikasi dapat mengenkripsi semua file dokumen, audio, video dan citra.Dan hasil yang didapat pada faktor penentu berhasil atau gagalnya enkripsi ternyata tidak tergantung dari format file melainkan dari ukuran file, semua ukuran file bisa kecuali GB. yaitu pada ukuran file yang besar dari ukuran file2,32 GB.

Kata Kunci: *Kriptografi, DES, Caesar Chiper, File Dokumen.*

1. PENDAHULUAN

Teknologi Komputer sebagai sarana penyimpanan dan pengiriman data, informasi, dan dokumen yang penting dan rahasia sering dapat dengan mudah diakses oleh orang yang tidak bertanggungjawab. keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Untuk itu, data, informasi dan dokumen perlu dilakukan pengamanan. Salah satu teknik pengamanan yang bisa dipelajari dan dikembangkan adalah kriptografi.

1. Salah satu bentuk pengamanan data adalah dengan cara mengenkripsi data tersebut agar tidak dapat dibaca orang lain yang tidak berhak. Dalam bidang Kriptografi

terdapat dua konsep yang sangat penting atau utama yaitu Enkripsi dan Deskripsi. Enkripsi adalah suatu proses yang melakukan perubahan dari yang bisa dimengerti menjadi tidak bisa dimengerti tidak terbaca.

2. Pada penelitian sebelumnya Ada banyak algoritma enkripsi yang bisa diterapkan untuk mengamankan data seperti DES, 3DES, RC4, AES dan lain-lain. Tetapi pada Jurnal ini akan dicoba Aplikasi untuk mengamankan data yaitu dengan menggabungkan dua algoritma lemah yaitu DES dan Caesar Chipher. Dan pada algoritma enkripsi dibuat untuk mengetahui tingkat keamanannya, sedangkan Deskripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Pada semua berkas file yang ada pada komputer yang dapat di enkripsi adalah file dokumen berupa berkas citra berformat Jpg, berkas audio berformat Mp3, atau dalam format lainnya seperti Txt, Pdf.
3. Berdasarkanuraiandiatas, akan dilakuakan penelitian membuat aplikasi dengan menggabungkan metode Aplikasi Kriptografi dengan MetodeEnkripsiFilemenggunakan Gabungan Algoritma Des Dan Caesar Chiper Untuk Keamanan Dokumen yang akan menghasilkan data yang lebih aman.

2. METODE

Landasan Teori

Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua proses yaitu melakukan enkripsi dan dekripsi (Munir,R,2006).

Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Sekarang bidang ilmu ini menjadi salah satu isu suatu topik riset yang tidak ada habis-habisnya diteliti dengan melibatkan banyak peneliti. Ilmu kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "Penyandian Transposisi" merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan.

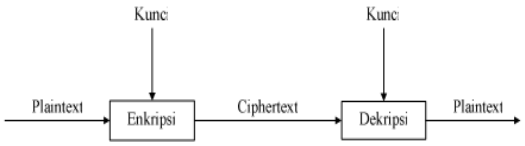
Kriptografi Klasik

Direkonstruksi Yunani kuno *scytale* (berima dengan "Italia"), sebuah perangkat awal sandi. Paling awal bentuk rahasia menulis dibutuhkan sedikit lebih dari pena lokal dan Analog kertas, karena kebanyakan orang tidak bisa membaca. Jenis *cipher* klasik utama adalah sandi transposisi, yang mengatur ulang susunan huruf dalam pesan (misalnya, "halo dunia" menjadi "owrdl ehlol" dalam penataan ulang skema sederhana trivial), dan *cipher* substitusi, yang secara sistematis menggantikan huruf atau kelompok huruf dengan surat-surat lain atau kelompok huruf (misalnya, "terbang sekaligus" menjadi "gmz podf bu" dengan mengganti setiap huruf dengan yang berikut dalam abjad latin).

Kunci Algoritma Kriptografi

Berdasarkan kunci yang dipakai, kunci algoritma kriptografi dapat dibedakan atas dua golongan, yaitu :

1) Kunci Simetris
2) Kunci Asimetris



Gambar 1. Proses enkripsi-deskripsi kunci simetris (Rinaldi Munir, 2006)

Gambar 2. Proses enkripsi-deskripsi kunci asimetris (Rinaldi Munir,2006)

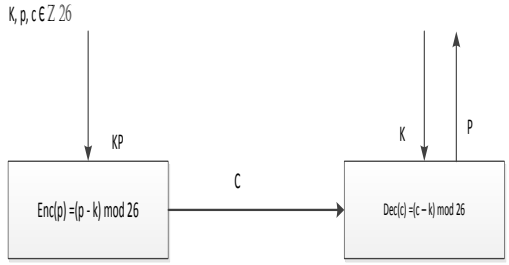
Caesar Cipher

Sejarah Caesar Chiper

Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan *cipher* substitusi untuk mengirim pesan ke *Marcus Tullius Cicero*. Pada *cipher* ini, huruf-huruf alfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. Karena hanya satu alfabet yang digunakan, *cipher* ini merupakan substitusi *monoalfabetik*. Sandi *Caesar* (sebutan dari *chiper)* merupakan system persandian klasik berbasis subtitusi yang sederhana. Enkripsi dan dekripsi pada system person dian *Caesar* menggunakan operasi *shift*. Operasi *shift* adalah mensubtitusi suatu huruf menjadi huruf pada daftar alphabet berada di-*k* sebelah kanan atau sebelah kiri huruf itu. Misalnya dipilih *k* =3 (ganti dengan huruf ke-3 sebelah kanan) maka"A" menjadi "D","B" menjadi "E" dan seterusnya. Bagaimana dengan "X","Y" dan "Z". Supaya semuanya memiliki subtitusi, huruf "A" dianggap disebelah kanan huruf "Z" sehingga "X" menjadi "A", "Y" menjadi "B" dan "Z" menjadi "C". Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table subtitusi :

Tabel 1. Substitusi

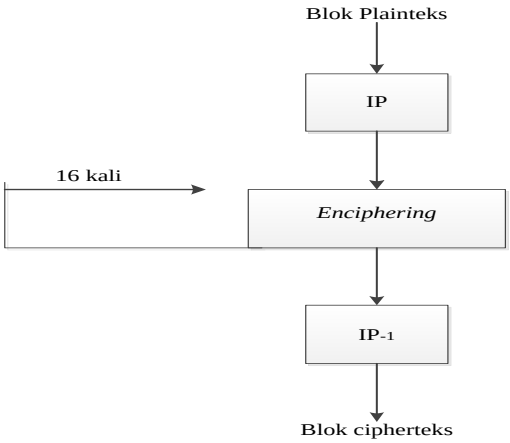
Plainteks :	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipherteks:	**D E F G H I J K L M N O P Q R S T U V W X Y Z A B C**



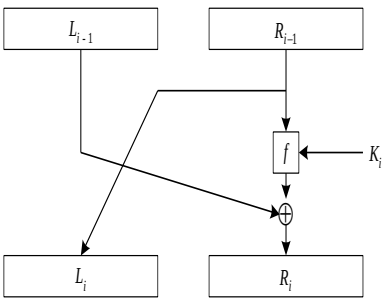
Gambar 3. Sandi Caesar (Rifki Sadikin,2012)

Pengertian Data Encryption Standard (DES)

Merupakan algoritma *cipher* blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, *AES*, karena *DES* sudah dianggap tidak aman lagi.



Gambar 4. Skema Global Algoritma DES (Rinaldi Munir,2006)



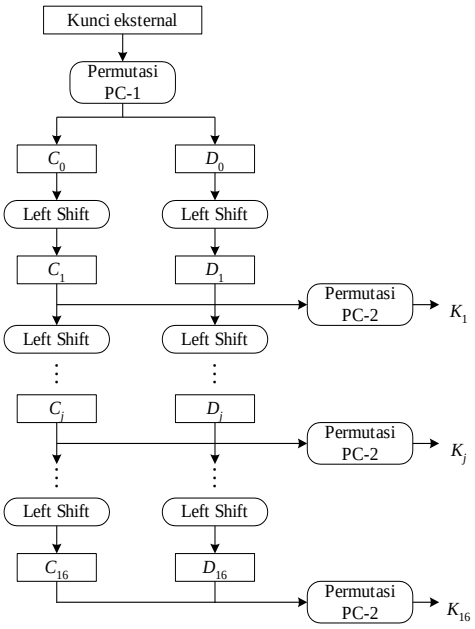
Gambar 5. Jaringan *Feistel* Untuk Satu Putaran DES

Permutasi Awal

Sebelum putaran pertama, terhadap blok plainteks dilakukan permutasi awal *(initial-permutation* atau *IP*). Tujuan permutasi awal adalah mengacak plainteks sehingga urutan bit-bit di dalamnya berubah.

Pembangkitan Kunci Internal

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K_1, K_2, ...,K_{16}. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.



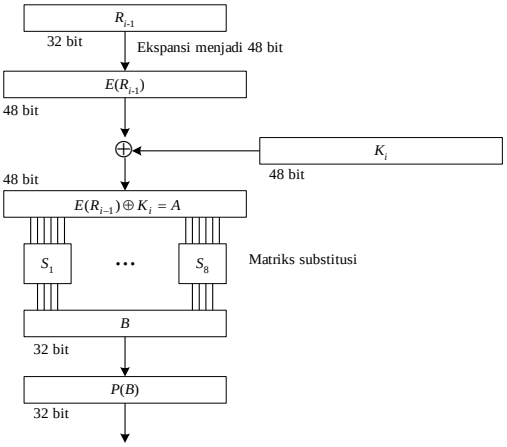
Gambar 6. Proses pembangkitan kunci-kunci internal DES

Enciphering

Proses *enciphering* terhadap blok plainteks dilakukan setelah permutasi awal (lihat Gambar 2.4). Setiap blok plainteks mengalami 16 kali putaran *enciphering*. Setiap putaran *enciphering* merupakan jaringan *Feistel* yang secara matematis dinyatakan sebagai

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

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



Gambar 7. Rincian Komputasi fungsi *f*

Permutasi Terakhir (*Inverse Initial Permutation*)

Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan.Proses permutasi menggunakan matriks permutasi awal balikan (*inverse initial permutation* atau IP^{-1})

Dekripsi

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K_1, K_2, …, K_{16}, maka pada proses dekripsi urutan kunci yang digunakan adalah K_{16}, K_{15}, …, K_1. Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran *deciphering* adalah

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

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

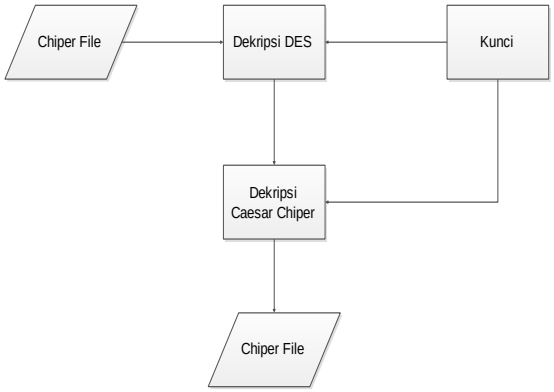
Mode *Data Encryption Standart* (DES)

DES dapat dioperasikan dengan mode ECB, CBC, OFB, dan CFB. Namun karena kesederhanaannya, mode ECB lebih sering digunakan pada paket program komersil.

Keamanan *Data Encryption Standart* (DES)

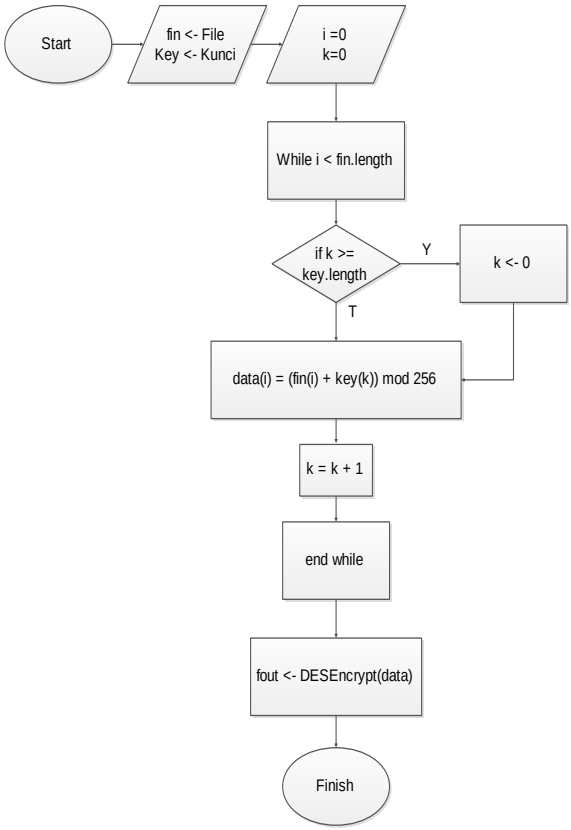
Keamanan Data Encryption Standart :

1) Panjang kunci
2) Jumlah Putaran
3) Kotak-S



Gambar 8. Proses Dekripsi

Algoritma Enkripsi Dan Dekripsi

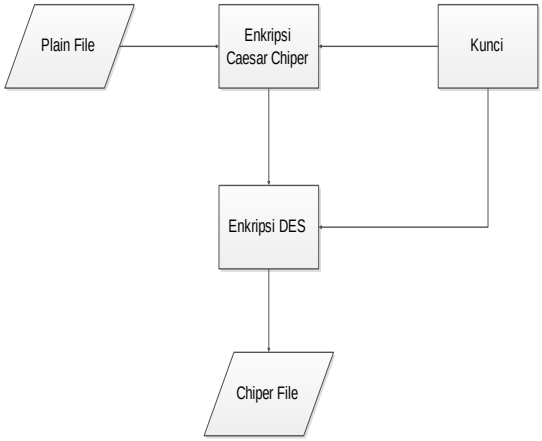


Gambar 9. Flowchart Enkripsi

3. HASIL DAN PEMBAHASAN

Perancangan Sistem

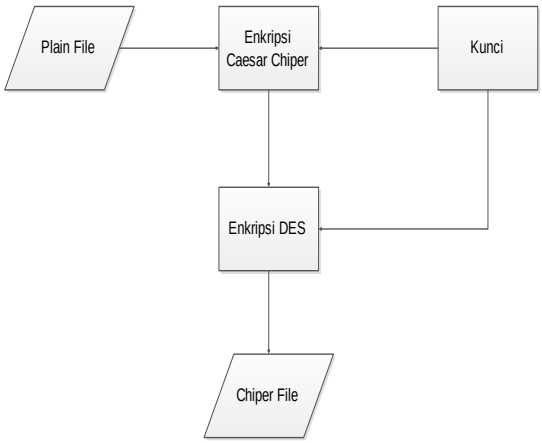
Konsep Aplikasi



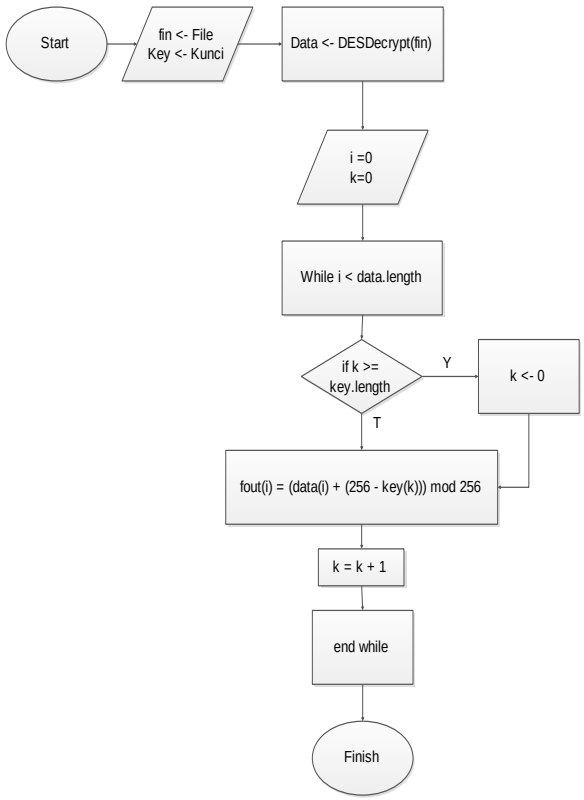
Gambar 10. Proses Enkripsi

Perancangan Sistem

Konsep Aplikasi



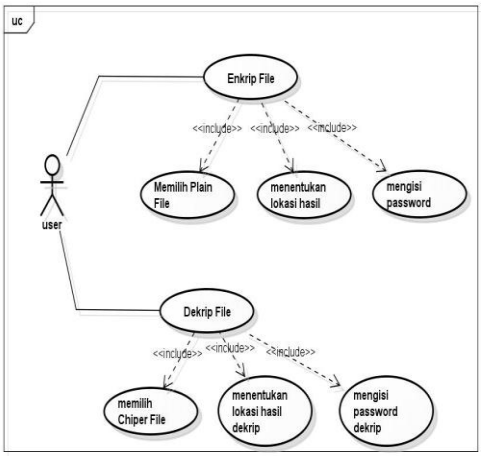
Gambar 11. Proses Enkripsi



Gambar 12. Flowchart Dekripsi

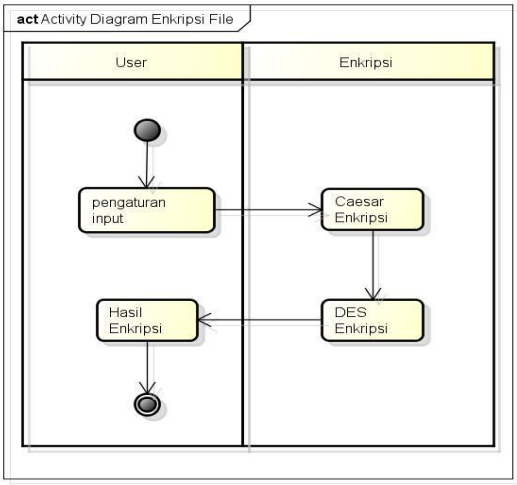
Perancangan Sistem Dalam Interaksi Dengan User

Use Case

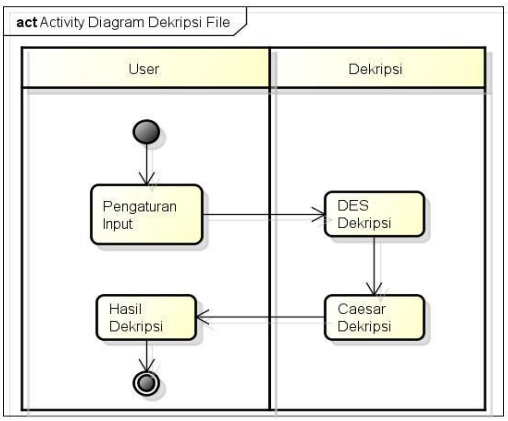


Gambar 13. Use Case

Aktivity Diagram

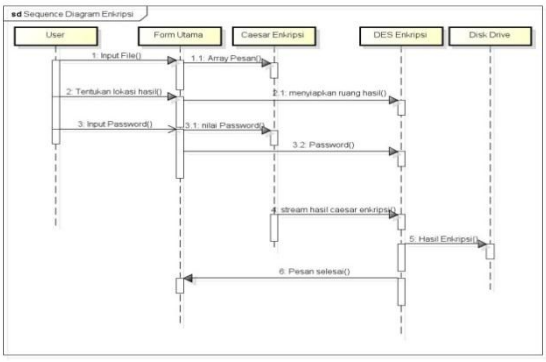


Gambar 14. Aktifity Diagram Enkripsi File

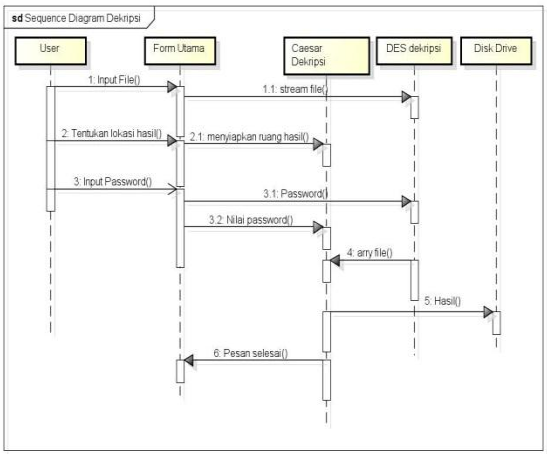


Gambar 15. Aktivity Diagram DekripsiFile

Sequence Diagram

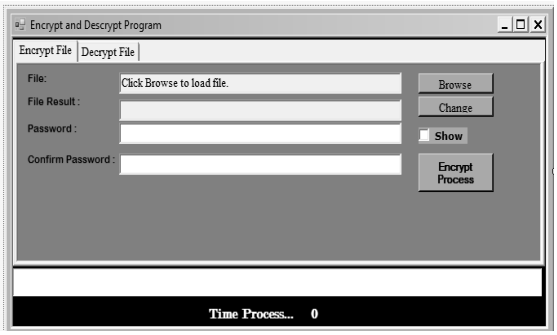


Gambar 16. Sequence Diagram Enkripsi

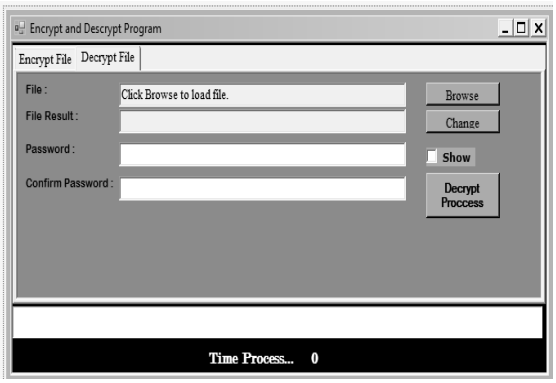


Gambar 17. Sequence Diagram Dekripsi

Desain Form



Gambar 18. Form Enkripsi



Gambar 19. Form Dekripsi

IMPLEMENTASI

Implementasi ini akan menjelaskan tentang hasil pengujian aplikasi program dan menjelaskan hardware dan juga software pendukung, untuk menjalankan aplikasi yang dibuat.

Lingkungan Pengembangan

Yang dimaksud lingkungan pengembangan pada bab ini adalah perangkat keras dan perangkat lunak yang digunakan dalam membuat aplikasi enkripsi seperti pada perancangan.

Lingkungan Perangkat Keras

Perangkat keras yang digunakan dalam pembuatan aplikasi enkripsi ini adalah:

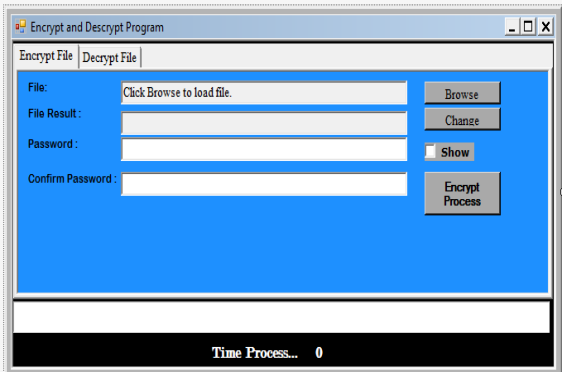
1. Prosesor Intel(R) Core(TM) i3 CPU M 370 @ 2.40GHz (4 CPUs), ~2.4GHz
2. Memori RAM 2,00 GB
3. Hardisk 42GB Free (320 GB Total)
4. Mouse
5. Keyboard

Lingkungan Perangkat Lunak

Perangkat lunak yang digunakan dalam pengembangan aplikasi kriptografi DES dan Caesar chiper ini adalah sebagai berikut:

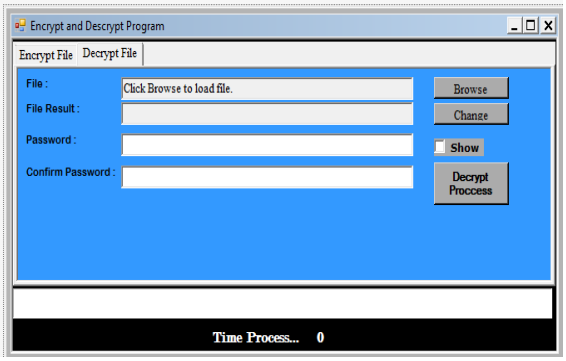
1. Sistem operasi : windows 7 Ultimate
2. Software Pendukung : Microsoft Visual Studio 2012

Tampilan Form Enkripsi File



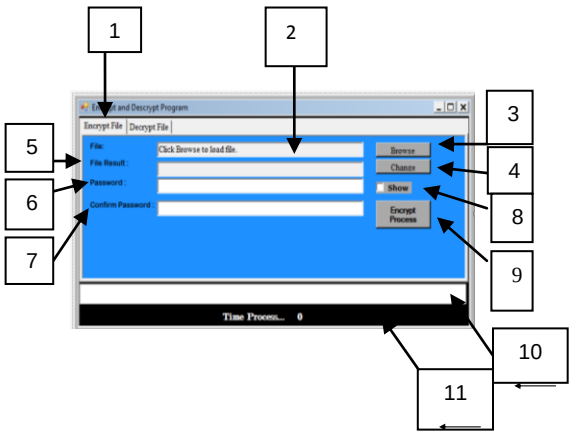
Gambar 20. Form Enkripsi File

Tampilan Form Dekripsi File



Gambar 21. Form Dekripsi File

Uji Coba



Gambar 22. Tampilan Form *Encrypt*

4. PENUTUP

Berdasarkan penelitian yang didapatkan aplikasi kriptografi dengan metode enkripsi file menggunakan gabungan algoritma Des dan Caesar cipher untuk keamanan dokumen dapat disimpulkan sebagai berikut:

1. Kriptografi untuk keamanan dokumen ini dapat dienkripsi dan didekripsi menggunakan gabungan algoritma Des dan Caesar cipher, yang dapat dienkripsi dan didekripsi yaitu semua isi file dokumen.
2. Kriptografi ini merupakan perangkat lunak untuk mengenkripsi dan dekripsi sebuah file dokumen agar tidak dapat dibaca oleh orang yang tidak berhak walaupun dengan melihat kode sumber programnya.

Saran

Kriptografi pada algoritma Des dan Caesar cipher untuk keamanan dokumen ini masih perlu dikembangkan lagi, saran untuk pengembangan lebih lanjut sistem ini sebagai berikut :

1. Untuk dapat menggabungkan algoritma Des dan Caesar cipher untuk keamanan dokumen seperti berkas citra berformat Jpg, audio berformat Mp3, video, dan format lainnya seperti Txt dan Pdf, maka perlu adanya Enkripsi dan Deskripsi.
2. Penggunaan algoritma kriptografi untuk mengenkripsi file dokumen, agar dapat mengkripsi gambar dan grafik dan format file lainnya.

5. DAFTAR PUSTAKA

[1] Hartini, Primaini.2014 *Kriptografi Password*. Palembang:Informatika Palembang Herryawan,I.P. 2010. *Aplikasi Keamanan Data Menggunakan Metode Kriptografi Gost*,Jurnal TSI, Vol. 1 No. 2.

[2] Munir, Rinaldi. 2006. *Kriptografi*. Bandung:Informatika Bandung

[3] Sadikin, Rifki. 2012. *Kriptografi Untuk Keamanan Jaringan*.Yogyakarta:Andi

[4] Yuswanto Dan Subari. 2007. *Pemrograman Database Visual Basic* .NET.Jakarta NIST,1995. *Data Encryption Standard*.

[5] Stalling, W,2006. *Cryptography And Network Security*. *(http://* en.wikipedia.org/wiki/*Cryptography.pdf*), diakses pada 15 juli 2012