IMPLEMENTASI ENKRIPSI DALAM PENGAMANAN FILE DATA KARYAWAN DENGAN METODE ALGORITMA *DES (DATA ENCRYPTION STANDARD)* PADA CV. SINERGI INFORMASI GLOBAL

Sabar Hanadwiputra
Program Studi D3 Komputerisasi Akuntansi, STMIK Bani Saleh
Email : sabar.hanadwiputra@gmail.com

Abstrak

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (message).Kripgorafi telah banyak diimplementasikan di banyak hal.Smart Card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti /dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi cipherteks diistilahkan dengan enkripsi. Sedang proses pengembalian pesan chiperteks menjadi plainteks diistilahkan dengan deskripsi. Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriptografi yang di kembangkan menggunakan algoritma simetri DES (Data Encryption Standard) dengan bahasa pemograman Java.DES menggunakan sandi blok kunci simetrik dengan ukuran blok 64 – bit dan ukuran kunci 56 – bit.

Kata Kunci: *Plainteks, Cipherteks, Kriptografi, Enkripsi dan Deskripsi.*

PENDAHULUAN

Keamanan data telah menjadi aspek yang sangat penting dalam suatu perusahaan. Data-data ini berisikan dokumen-dokumen penting perusahaan tersebut yang mana harus bersifat rahasia dan tertutup.Tetapi data tersebut bisa di ubah ataupun di rusak oleh pihak yang tidak bertanggung jawab baik itu dari

pihak luar maupun dari pihak dalam.Untuk itu sangat penting dilakukan pengamanan data.Salah satu upaya pengamanan data pada sistem informasi yang dapat dilakukan adalah kriptografi.

Banyak sekali teknik kriptografi yang dapat digunakan untuk mengenkripsi dan deskripsi data. Salah satu teknik yang dipergunakan dalam kriptografi adalah metode DES (*Data Encryption Standard*). Metode *DES* merupakan metode yang paling banyak digunakan di dunia, yang di adopsi oleh NIST (*National Institute of Standard and Technology*) sebagai standar pengolahan informasi federal AS. DES (*Data Encryption Standard*) merupakan algoritma *cipher* blok yang popular karena dijadikan standar algoritma enkripsi kunci-simetri. Secara umum *DES* terbagi menjadi tiga kelompok yaitu pemrosesan kunci, enkripsi data 64 bit dan deskripsi data 64 bit yang mana satu kelompok saling berintegrasi satu sama lain.

Jika file data master perusahaan terlindungi oleh sistem keamanan, maka data tersebut aman karena data tersebut tidak bisa sembarangan di ubah tetapimisalnya jika ada pegawai atau orang luar yang menggunakan komputer tersebut selain dari user nya maka dia dapat melakukan manipulasi data yang fiktif dari master data yang sudah ada, maka data tersebut akan masuk kedalam laporan dan karyawan

perusahaan akan membuat laporan tersebut ataupun laporan tersebut langsung akan direalisasikan. Ketika saat pelaporan data hasil ke manager, terjadi ketidaksamaan hasil yang diharapkan manager karena data master yang di berikan oleh manager berbeda dengan data yang ada pada komputer karyawan tersebut.

METODOLOGI PENELITIAN

Kegiatan penelitian ini direalisasikan dalam beberapa tahapan berikut:

1. Studi Literatur. Pencarian dan pengumpulan literatur-literatur dan kajian-kajian yang berkaitan dengan masalah-masalah yang ada, baik berupa artikel, jurnal nasional dan internasional.
2. Buku referensi, internet dan sumber-sumber lain yang berhubungan dengan masalah.
3. Perumusan Masalah Dengan menganalisa semua permasalahan yang ada berdasarkan pengamatan terhadap masalah dan sumber yang ada.
4. Desain dan Perancangan Berisi penjelasan mulai dari proses desain hingga konfigurasi untuk implementasi sistem, serta skenario yang digunakan untuk melakukan pengujian.
5. Implementasi dan Analisis Melakukan analisis terhadap data-data yang telah diperoleh pada saat tahap implementasi dan pengumpulan data.

1.1 Kemanan komputer

Keamanan komputer adalah kumpulan peranti yang dirancang untuk melindungi komputer sehingga data pada komputer terlindungi dari pengganggu yang tidak dikenali dalam sistem komputer. (Stalling, 2012).

Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.(John D. Howard, "An Analysis of security incidents on the internet",1999).

Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan penggangu yang tidak dikenali dalam system komputer.(Gollmann, "Computer Security", 1999).

1.2 Kritografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*.*Crypto* berarti*ecret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain.(Ariyus, 2008).

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut *BruceScheiner* dalam bukunya "*Applied Chryptography"*, kriptografi adalah ilmu pengetahuan dan seni menjaga pesan – pesan agar tetap aman (*secure*).

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi.Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu.Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan.Untuk melaksanakan tujuan tersebutlah dirancang suatu

sistem keamanan yang berfungsi melindungi sistem informasi.

Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan.

2.3 Mekanisme Kriptografi

Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekkannya dengan cara yang sangat primitif.

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi.

1. ***Plaintext***

   Plaintext (message) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.

2. ***Chipertext***

   Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.

3. ***Chiper***

   Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.

4. ***Enkripsi***

   Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.

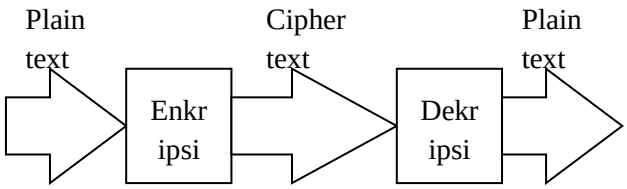
5. ***Dekripsi***

   Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.

6. ***Kriptosistem***

   Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Urutan-urutan proses kriptografi dapat digambarkan sebagai berikut.



Gambar 2.1 Mekanisme Kriptografi

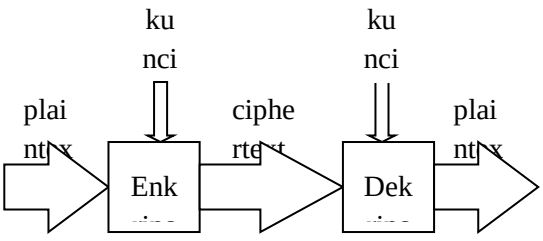
Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali

plaintext (m). Secara matematis proses ini dapat dinyatakan sebagai,

$$E(m) = c$$
$$D(c) = m$$
$$D(E(m)) = m$$

Kriptografi sederhana seperti ini menggunakan algoritma penyandian yang disebut *cipher*.Keamanannya bergantung pada kerahasiaan algoritma penyandian tersebut, karena itu algoritmanya harus dirahasiakan. Pada kelompok dengan jumlah besar dan anggota yang senantiasa berubah, penggunaannya akan menimbulkan masalah. Setiap ada anggota yang meninggalkan kelompok, algoritma harus diganti karena anggota ini dapat saja membocorkan algoritma.

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dengan demikian ada sedikit perubahan yang harus dilakukan pada mekanisme yang digambarkan pada gambar 2.1 menjadi seperti gambar 2.2 berikut ini.



Gambar 2.2 Kriptografi berbasis kunci

Mekanisme kriptografi seperti ini dinamakan kriptografi berbasis kunci. Dengan demikian kriptosistemnya akan terdiri atas algoritma dan kunci, beserta segala plaintext dan ciphertextnya.

Persamaan matematisnya menjadi seperti berikut,

$$E_e(m) = c$$
$$D_d(c) = m$$
$$D_d(E_e(m)) = m$$

dengan,

e = kunci enkripsi ;d = kunci dekripsi

2. IMPLEMNTASI DAN PEMBAHASAN

Data Encryption Standard (DES)

DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit (8 karakter) plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key). Kunci internaldibangkitkan dari kunci eksternal (eksternal key) yang panjangnya 64 bit.

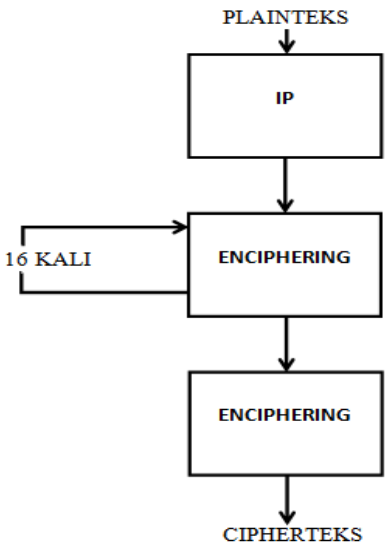
DES termasuk kedalam sistem kriptografi simetri dan tergolong jenis cipher blok. Skema global metode DES adalah sebagai berikut :

I. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
II. Hasil permutasi awal kemudian di-enciphering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
III. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (*invers*

permutation atau IP^{-1}) menjadi blok cipherteks.

IV. 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.

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



Gambar 2.5 Skema Global Metode DES

Implikasi Penelitian

Pada proses tahap ini dilakukan implementasi dan pengujian hasil dalam bentuk langkah – langkah konfigurasi berdasarkan hasil observasi lapangan.

Proses Pembentukan Kunci Kunci Data Encryption Standard (DES)
Kunci internal.

Tabel 2.1 DES Kunci Internal

K	U	N	I	N	G	A	N
4B	55	4E	49	4E	47	41	4E
0100 1011	0101 0101	0100 1110	0100 1001	0100 1110	0100 0111	0100 0001	0100 1110
8	16	24	32	40	48	56	64

kunci eksternal :

Tabel 2.2 Kunci Eksternal

K	O	M	P	U	T	E	R
59	4F	47	49	52	45	4E	4F
0101	0100	0100	0100	0101	0100	0100	0100
1001	1111	0111	1001	0010	0101	1110	1111
8	16	24	32	40	48	56	64

Setelah dilakukan putaran sebanyak 16 kali putaran, hasil dari L[16] dan R[16], kemudian dilakukan Final Permuted (FP), sesuai dengan ketentuan tabel, berikut merupakan tabel FP :

Tabel 2.3 FP

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Hasilnya di dapat dari Final Permuted (FP), kemudian dilakukan kembali konversi ke hexadecimal. Kemudian konversi ke biner, berikut merupakan hasilnya :

Tabel 2.4 Hasil FP

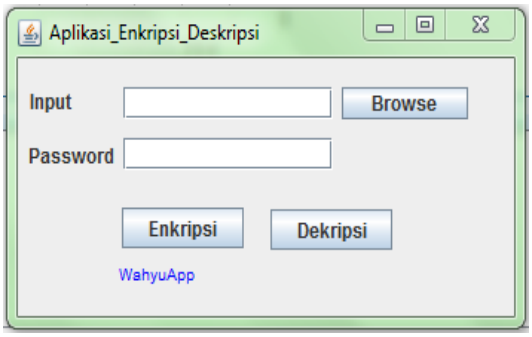
011110	110001	111101	001100	100000	010110	000101	110101
11	01	00	00	10	11	01	01
7 B	C 5	F 4	3 0	8 2	5 B	1 5	D 5
{	A	Ö	0	,	[	}	Ö

Hasil enkripsi menggunakan kunci internal KUNINGAN dari kunci eksternal KOMPUTER setelah dilakukan enkripsi sebanyak 16 putaran, hasilnya adalah {äc0,[Ö}.

Uji Perangkat Lunak

1. Tampilan Halaman Utama

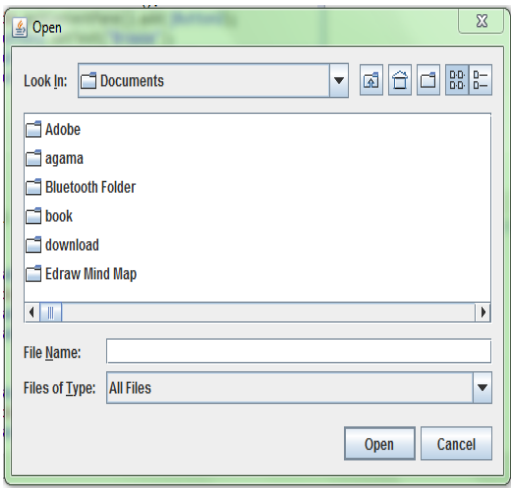
Pada tampilan halaman utama ini, penulis menyisipkan tombol Encrypt File dan Decrypt File, guna untuk memproteksi atau membuka proteksi data dan file di dalam computer, selanjutnya ada tombol Browse yang berguna untuk memilih file mana yang akan di enkripsi . Berikut merupakan tampilan halaman utama :



Gambar 2.4 Menu Utama

2. Tampilkan Halaman Pilih File

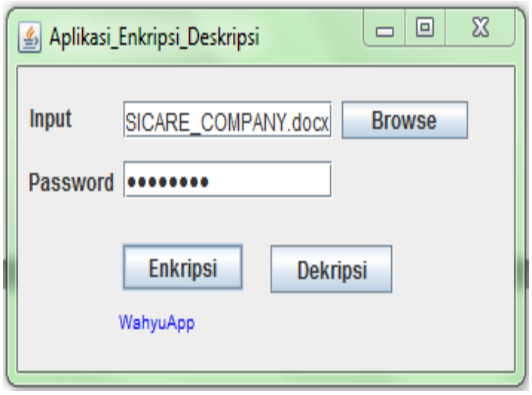
Tampilan pilih file ini berguna untuk memudahkan user untuk memilih file untuk di Encrypt File dan Decrypt File. Berikut merupakan tampilan pilih file :



Gambar 2.5 Menu File

3. Tampilan Halaman Membuat Password

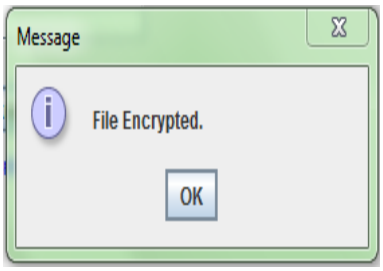
Setelah kita pilih file yang akan di enkrip, masuk ke input dan kita masukkan password yang kita inginkan.Tampilan membuat password ini berguna untuk mengencrpyt file yang sifatnya opsional, dalam hal ini pengisian password akan di baca sebagai input untuk kunci yang berpengaruh pada proses enkripsi. Berikut merupakan tampilan membuat Password :



Gambar 2.6 Membuat Password

4. Tampilan Message Enkrip

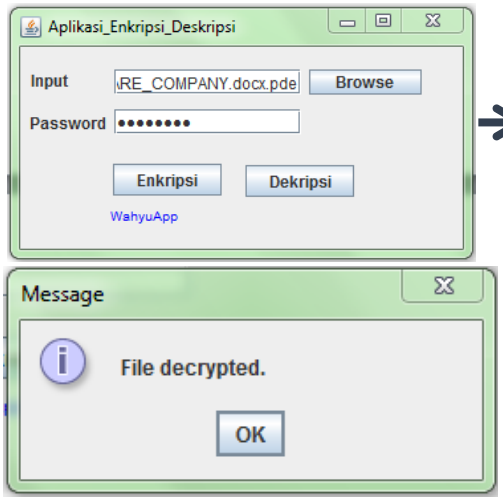
Setelah kita masukan password , lalu kita klik tombol enkripsi. Maka akan muncul Message Dialog bahwa file tersebut telah di enkripsi. Berikut merupakan tampilan Message Enkrip :



Gambar 2.7 Message Dialog Enkrip

5. Tampilan Message Decrypt

Setelah file tersebut di enkripsi, untuk mengembalikannya yaitu pilih kembali file yang tadi kita encrypt –> masukkan password yang sama sesuai dengan password enkrip –> lalu klik tombol decrypt. Maka akan mucul Message Dialog bahwa file tersebut telah di decrypt. Berikut merupakan tampilan Message Decrypt :



Gambar 2.8 Tampilan Message Decrypt

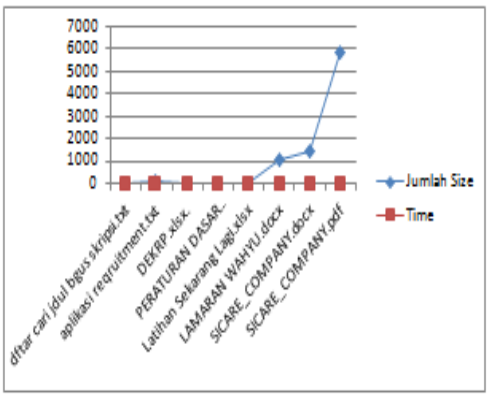
Pengujian*Response Time* Enkripsi dan Dekripsi

Dalam percobaan *response time* proses enkripsi dan dekripsi, penulis menentukan dengan kunci yang sama yaitu

Kunci : wahyu212

Tabel 2.5 Pengujian *Response Time* Proses Enkripsi

Jumlah Size	Nama File	Response Time
1 kb	dftar cari jdul bgus skripsi.txt	21 sec
124 kb	aplikasi reqruitment.txt	22 sec
15 kb	DEKRP.xlsx.	23 sec
30 kb	PERATURAN DASAR PERUSAHAA1.docx.	25 sec
26 kb	Latihan Sekarang Lagi.xlsx	26 sec
1,050 kb	LAMARAN WAHYU.docx	27 sec
1,412 kb	SICARE_COMPANY.docx	28 sec
5,894 kb	SICARE_COMPANY.pdf	30 sec



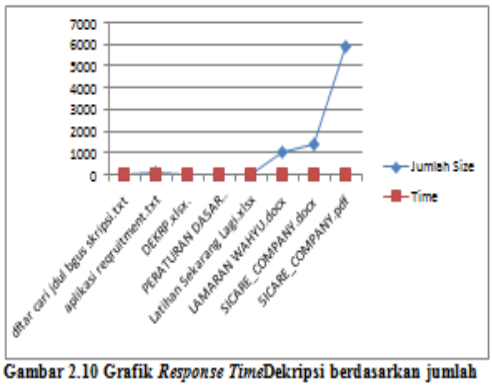
Gambar 2.9 Grafik *Response Time* enkripsi berdasarkan jumlah size

Dari percobaan tersebut pada tabel 2.5 dan gambar 2.9 diperoleh response time

rata-rata proses enkripsi adalah 0.02362 detik size

Tabel 2.6 Pengujian *Response Time* Proses Dekripsi

Jumlah Size	Nama File	Response Time
1 kb	diftar cari jdul bgus skripsi.txt	23 sec
124 kb	aplikasi reqruitment.txt	23 sec
1 kb	DEKRP.xlsx.	23 sec
30 kb	PERATURAN DASAR PERUSAHAA1.docx.	24 sec
26 kb	Latihan Sekarang Lagi.xlsx	26 sec
1,050 kb	LAMARAN WAHYU.docx	27 sec
1,412 kb	SICARE_COMPANY.docx	22 sec
5,894 kb	SICARE_COMPANY.pdf	31 sec



Gambar 2.10 Grafik *Response Time*Dekripsi berdasarkan jumlah karakter size

Dari percobaan tersebut pada tabel 2.6 dan gambar 2.10 diperoleh *response time* rata-rata proses dekripsi adalah 0.023269 detik per size.

Pada percobaan data *response time* diatas penulis menyimpulkan bahwa semakin banyak jumlah size yang dienkripsi dan didekripsi maka akan semakin lama waktu yang diperlukan.

3. KESIMPULAN

Berdasarkan dari hasil proses implementasi, pengujian, dan analisis dapat ditarik kesimpulan sebagai berikut:

a. Dengan adanya sistem keamanan ini diharapkan dapat memberikan rasa aman bagi karyawan dalam penyimpanan data perusahaan.
b. Aplikasi pengamanan file ini merupakan aplikasi yang berfungsi untuk melakukan enkripsi dan deskripsi data dengan metode DES pada jenis file tertentu sehingga data tidak mudah diketahui orang.
c. Tidak ada lagi kesalahan ketika penyerahan laporan kepada manager karena master data terlindungi.
d. Meningkatnya kualitas keamanan data perusahaan memberikan dampak positif bagi perusahaan yaitu bertambahnya klien dari perusahaan lain yang datang untuk bekerjasama dengan perusahaan ini karena keamanan datanya baik.
e. Semakin besar jumlah size pada suatu file yang akan di enkripsi maka akan semakin lama juga running time pada aplikasi pengamanan file ini tergantung dari isi dan jenis file itu sendiri.

DAFTAR PUSTAKA

Andri, M Yuli (2009).Implementasi Algoritma Kriptografi DES, RSA dan Algoritma Kompresi LZW pada berkas Digital. Universitas Sumatra Utara : Skripsi

Ariyus.D.(2008).Pengantar Ilmu Krptografi.Yogyakarta : Andi Offset
System Development Life Cycle (2017, September Senin) Di ambil dari thesis.binus.ac.id

Irmawati (2016).Pengembangan aplikasi kriptografi file dokumen, audio dan gambar dengan algoritma DES. Jurnal Volume VIII, No 2, irmawati@civitas.unas.ac.id.

Karya, Yogi (2013). Enkripsi dengan Algoritma DES (Data Encryption Standard) untuk keamanan file.

Primartha, Rifkie, (2011). Penerapan enkripsi dan deskripsi file menggunakan algoritma Data Encryption Standard (DES). Jurnal Volume 3, No 2,

http://ejournal.unsri.ac.id/index.php/jsi/index

Shofi, Ahmad (2016). Enkripsi dan deskripsi dengan metode Data Encryption Standard (DES) dengan menggunakan bahasa pemograman PHP.

Stalling(2012). Keamanan Komputer. Dalam R. Sadikin, Kriptografi untuk keamanan jaringan (hal.1). Yogyakarta: Andi Offset.