APLIKASI KEAMANAN EMAIL MENGGUNAKAN ALGORITMA EOF DAN RC4

Dimas Parissuhelmi[1)], Subandi, M.Kom[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : dimasparissuhelmi@gmail.com[1)], subandionline@gmail.com[2)]

ABSTRAK

Informasi ialah sebuah hal yang sangat dibutuhkan dari zaman dulu. Dari sejenis picture, voice, file maupun tulisan. Informasi dapat berfungsi untuk seseorang yang mempunyai hak menggunakannya. Lain halnya dapat menimbulkan kesalahan bila diketahui seseorang yang tidak mau menanggung resikonya. Dari pertukaran informasi saat sekarang ini yang maju dengan pesat membuahkan informasi seseorang menjadi enggan untuk dicuri dan yang sangat pesat terlihat ialah dalam kehidupan dunia maya. Email ialah sebuah teknologi yang sangat dikagumi seseorang sekarang ini. Dengan memakai email kita tidak akan kesulitan lagi jalan ke tempat pengiriman surat atau tempat pengiriman lainnya untuk mengirim sebuah informasi. Email ini memberi kepuasan yang amat sangat memadai sehingga kita dapat mengirim file yang penting dalam dunia maya. Kita bisa juga tidak harus menemui si penerima informasi. Sebab ini yang menjadi alasan P.T. Murti Indah Sentosa memakai email untuk media pertukaran informasi.

Kata Kunci: Steganografi, *EOF*, Kriptografi, *Rivest Code 4*, Email

1. PENDAHULUAN

Dunia teknologi informasi yang berkembang cepat dan membawa banyak perubahan dalam kehidupan manusia. Banyak berbagai cara yang dilakukan manusia untuk menyimpan dan menjaga keutuhan informasi dari pihak atau orang lain yang tidak mempunyai hak. Sebagai contoh, yaitu P.T. Murti Indah Sentosa yang bergerak di bidang penyediaan dan perbaikan alat kesehatan, supaya lebih mudah, dokumen-dokumen penting seperti surat penawaran, faktur pemesanan, slip gaji karyawan, surat keputusan dan *file-file* lainnya yang dikirimkan melalui *email* ini memerlukan keamanan yang dikirimkan melalui *email*. Guna untuk menjaga serta memenuhi tuntutan keamanan dan integritas suatu data atau infromasi terhadap pihak-pihak yang tidak bertanggung jawab. Di perusahaan distributor alat kesehatan seperti P.T. Murti Indah Sentosa ini, informasi yang diterima atau dikirim melalui *email* merupakan salah satu data yang paling penting. Maka dari itu, dibutuhkan sebuah metode yang bisa menjaga keamanan informasi tersebut. Metode yang dimaksud ialah kriptografi dan steganografi yang mempunyai maksud suatu seni dan bidang keilmuan juga penyediaan informasi atau suatu pesan yang bertujuan menjaga kerahasiaannya. Walau saja sudah berkembang dari zaman dulu, teknik kriptografi yang dibutuhkan masa kini tetap harus mengikuti dirinya terhadap menyebarnya penggunaan komputer digital pada masa kini. Dalam perkembangan teknologi saat ini, teknologi *email* (*Electronic Mail*) ialah merupakan suatu teknologi yang sangat diinginkan dan amat sangat penting di dalam dunia informasi. Dari adanya *email*, manusia bisa mengirim pesan dan juga data melalui teknologi informasi. Dari zaman teknologi yang mengembang pesat, pengiriman pesan melalui tempat pengiriman pesan sudah sangat jarang dipergunakan. Hal ini karena pengiriman melalui tempat pengiriman pesan butuh waktu yang amat sangat lama dan proses yang kurang efisien. Faktor inil yang membuat kuat manfaat *email* dalam kehidupan kita. Pengiriman pesan secara tradisional atau melalui tempat pengiriman pesan masih digunakan untuk berkomunikasi yang bersikap formal, seperti antar kantor pemerintah dan dunia pendidikan. Namun, kadang banyak seseorang yang berbalik ke dalam penggunaan *email* untuk pengiriman pesan formal dikarenakan lebih mudah dan cepat. Namun, selain macam-macam keuntungan dan kepraktisan yang diberikan dari teknologi tersebut, mungkin saja potensi bahaya yang akan muncul. Contohnya ialah terjadinya kejadian seperti kebocoran data atau informasi yang diterjemahkan. Kebocoran data ini akan mungkin terjadi karena terkirimnya *email* melalui internet akan melalui proses yang amat panjang yaitu melewati banyak *server*. Dan dirusak oleh adanya *hacker* yang menyelinap melalui akun *email* agar mendapatkan suatu informasi dari akun tersebut. Maka dari itu, perlu diadakan sebuah enkripsi yaitu dengan sebuah keamanan *email* untuk melakukan kerusakan pesan dan data dalam sebuah *email.* Pengamanan ini dilakukan untuk menghindari pembacaan oleh seseorang yang tidak bertanggung jawab, kecuali pada seseorang yang berhak mendapatkannya.

2. LANDASAN TEORI

Secara umum arti dari kata kriptografi ialah pesan rahasia. Kriptografi pada umumnya dijelaskan sebagai ilmu yang mempelajari cara menyisipkan tulisan. Kriptografi ialah sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf karakter di luar bentuk aslinya, (Nurhardian & Ahmad Pudoli) [1].

Secara garis besarnya, kriptografi yaitu teknik pengamanan informasi yang dijalani menggunakan cara pengolahan informasi awal *(plaintext)* menggunakan sebuah kunci tertentu dengan sebuah metode enkripsi tertentu sehingga membuahkan hasil sebuah informasi baru *(chipertext)* yang tidak bisa dibaca dengan detail. *Chipertext* tersebut bisa diputar balik lagi menjadi informasi awal *(plaintext)* melalui proses dekripsi. Kriptografi ialah suatu bidang ilmu yang dapat menjadi solusi dari sebuah masalah keamanan data.

Keamanan dari sebuah kriptografi diposisikan pada kerahasiaan kunci. Lain halnya dengan algoritma kriptografi asumsi diketahui oleh semua orang secara umum. Sistem kriptografi yang amat sangat kuat mempunyai kemungkinan jangkauan kunci yang amat sangat besar sehingga sistem tidak bisa diselesaikan dengan mencoba semua kemungkinan kunci secara *bruteforce*, sistem kriptografi yang kuat juga menciptakan *chipertext* yang acak untuk semua standar statistik.

2.1 Tujuan Kriptografi

Aspek-aspek keamanan didalam kriptografi adalah :

1) *Confidentiality*(Kerahasiaan)
   Pelayanan yang ditunjukkan untuk menjaga supaya pesan tidak bisa dibaca oleh orang-orang yang tidak mempunyai hak.
2) *Data Integrity* (Integritas)
   Pelayanan yang menjamin bahwa pesan masih asli ataupun belum pernah dimanipulasi selama pengiriman.
3) *Authencitacion* (otentikasi)
   Layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authencitation* atau *entity authencitation*) maupun mengidentifikasi kebenaran sumber pesan (*origin authencitation*).
4) *Non-repudiation*(penyangkalan)
   Dimana suatu layanan untuk mencegah entitas yang berkomunikasi untuk melakukan penyangkalan, yaitu pengirim pesan dapat menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2 Konsep Dasar Dan Bagian Kriptografi

1) *Plaintext* merupakan teks asli yang dapat ditulis atau diketik yang hanya memiliki makna teks asli. Dimana yang akan diproses menggunakan algoritma kriptografi menjadi *chipertext.*
2) *Chipertext* dapat merupakan suatu pesan yang telah melalui proses yang tealah di enkripsi. Pesan yang ada dalam teks pengkodean ini tidak bisa dibaca karena berupa karakter-karakter yang yang tidak mempunyai makna tertentu.
3) *Enkripsi* adalah hal penting dalam kriptografi, merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya, enkripsi dapat diartikan juga sebagai penyandian data. *Plaintext* (pesan asli) diubah menjadi kode-kode yang tidak dimengerti (*Chipertex*). Enkripsi dapat dilakukan dengan menggunakan algoritma kriptografi tertentu.
4) *Dekripsi* merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi (*Chipertext*) dikembalikan ke bentuk asalnya (*Plaintext*). Dekripsi merupakan proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya.
5) Kunci *(key)* adalah kunci yang dipakai untuk melakukan proses enkripsi dan dekripsi.
6) Kriptanalis (*Cryptanalysis*), bisa diartikan sebagai analisis kode atau ilmu untuk mendapatkan *plaintext* (teks asli) tanpa harus mengetahui kunci. Hal ini dilakukan oleh kriptanalis. Ilmu ini juga dapat menemukan kelemahan dari suatu algoritma kriptografi dan akhirnya dapat menggunakan dapat menemukan kunci atau *plaintext* dari *chipertext* yang telah dienkripsi dengan algotima tertentu.

RC4 didesain oleh Ron Rivest yang berasal dari RSA *Security* pada tahun 1987 (Ariyanto, 2009). RC mempunyai singkatan resmi yaitu "*RivestChiper*", namun juga dapat dikenal sebagai "*Ron'sCode*" RC4 sebenarnya dirahasiakan dan tidak dipublikasikan, namun ternyata ada beberapa orang yang tidak dikenal menyebarkan RC4 ke *mailinglist Cypherpunks*. Kemudian berita ini dengan cepat dipublikasikan ke sci.crypt *newsgroup*, dan dari beberapa *newsgroup* ini kemudian menyebar luaskan di internet. Kode yang telah disebarkan tersebut dapat dipastikan keasliannya karena *output* yang dikeluarkan sama dengan *software-software* yang menggunakan RC4 yang berlisensi tersebut.

Nama RC4 yang sudah dipatenkan, sehingga RC4 dapat sering disebut juga ARCFOUR atau ARC4 (*Alleged* RC4) untuk menghindari masalah pematenan.

RSA *Security* tidak akan pernah secara resmi merilis algoritma tersebut, namun *Rivest* secara pribadilah yang merilisnya tersebut dengan menhubungkan *Wikipedia* Inggris ke catatan-catatan yang ia punya. RC4 telah menjadi bagian dari protokol

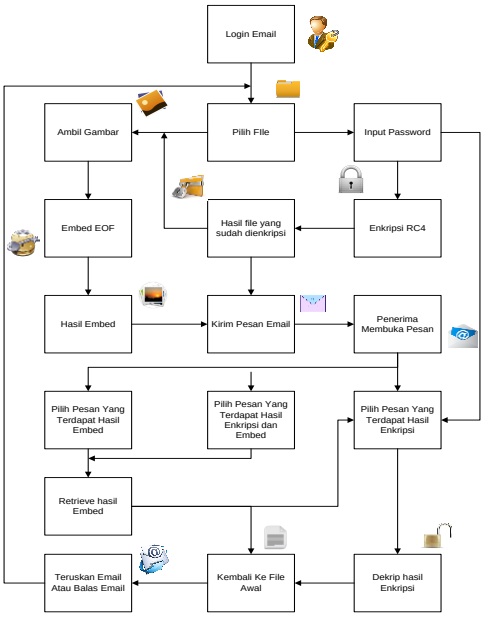
enkripsi yang standard dan sering digunakan, termasuk WEP dan WPA untuk wireless card, serta TLS.

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Skema Proses Keseluruhan Aplikasi

Enkripsi adalah proses pengacakan sebuah *file* dan *embed* adalah penyisipan *file* ke dalam gambar. Algoritma yang digunakan pada aplikasi ini adalah algoritma simetris RC4 yang akan mengenkrip *file* dan akan disisipkan ke dalam gambar menggunakan teknik steganografi EOF. Proses keseluruhan aplikasi ini dapat diuraikan sebagai berikut:

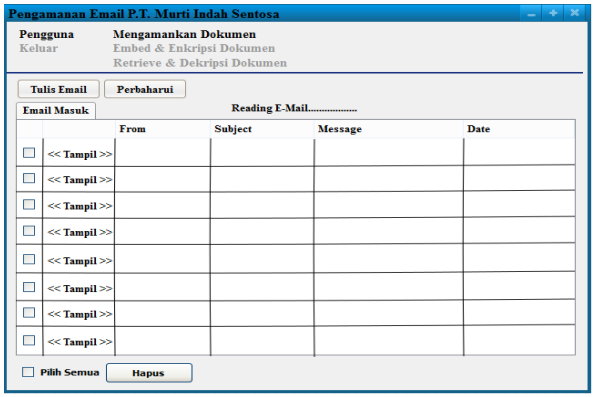
a. Memerlukan *input*an berupa *file*, *password*, dan gambar.
b. *User* harus *login* dengan *email* sendiri terlebih dahulu.
c. Pilih Tulis *Email* untuk mengirim pesan.
d. Lalu *user* memasukkan *email* penerima dan subject beserta isi pesan.
e. Setelah itu *user* dapat melampirkan dokumen-dokumen, ketika *user* melampirkan dokumen-dokumen tersebut, akan muncul *form* untuk *embed* dan enkripsi, proses pertama yang dilakukan *user* adalah harus memilih *file* untuk di enkripsi kemudian ceklis proses enkripsi.
f. Setelah itu *user* memilih *file* berupa gambar.
g. Lalu *user* memasukan *password* untuk enkripsi.
h. *File* yang telah terenkrip akan disisipkan ke dalam sebuah gambar.
i. Gambar yang ter*embed* akan ada penanda pesan pada akhir *byte* gambar.
j. Jika penerima sudah mempunyai aplikasi ini, penerima dapat *retrieve* dan dekripsi dokumen tersebut. Dengan menggunakan cara membuka pesan yang terdapat lampiran dalam dokumen berupa gambar.
k. Kemudian penerima dapat menyimpan *file* tersebut, jika *file* tersisip secara otomatis program akan membaca dokumen apabila tersisipi *file* lain, penerima harus memasukkan *password* apabila terdapat enkripsi di sebuah *file*.
l. Jika *file* yang telah melakukan enkrip dan *embed* akan kembali seperti *file* awalnya.
m. Penerima dapat pilih atau meneruskan, jika penerima ingin meneruskan pesan, atau dapat memilih balasan untuk membalas pesan tersebut. Jika diperlukan pengenkripsian atau pengdekripsian *file* dapat kembali untuk mengulangi langkah E tersebut.



Gambar 1: Rich Picture Proses Aplikasi

3.2 Rancangan Layar *Form* Menu Utama

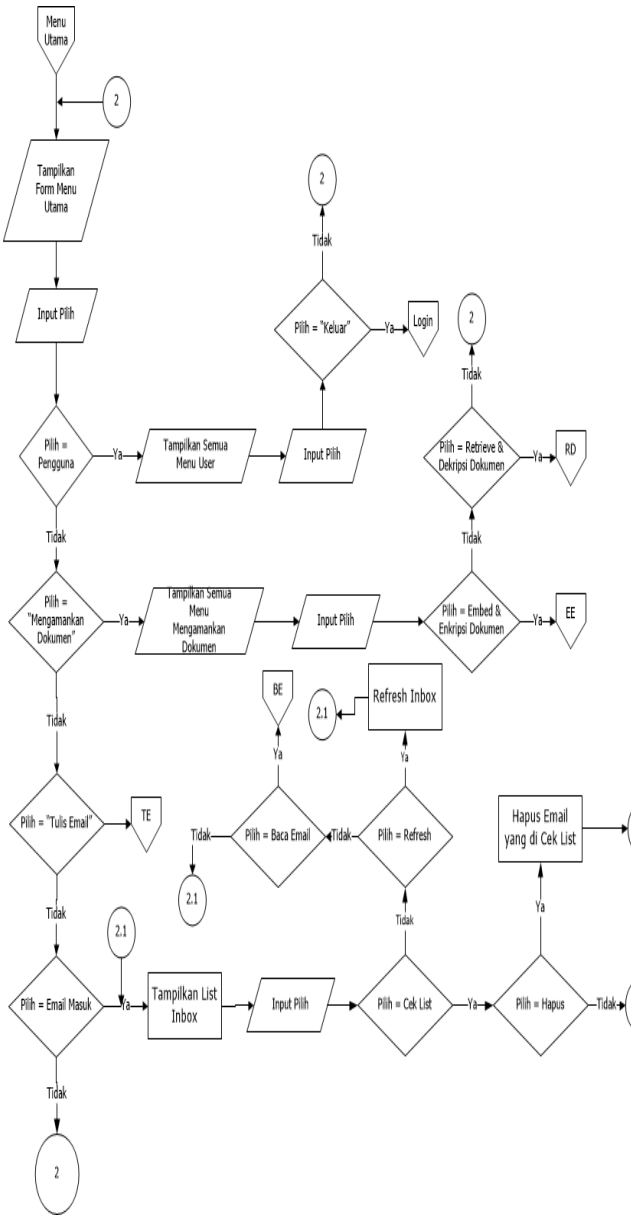
Setelah *Login* berhasil, pengguna masuk ke dalam *Menu* Utama. Di dalam *Menu* Utama ini, terdapat *Menu* Pengguna yang mempunyai *submenu Logout*, juga terdapat *Menu Email*, juga terdapat *Menu* Enkripsi yang mempunyai *submenu* Enkripsi Pesan, Enkripsi *File*, Dekripsi Pesan, Dekripsi *File*, dan *Menu* Tentang yang mempunyai *submenu* Tentang Sistem dan Tentang Pembuat. Pengguna bisa memilih *menu* dan *submenu* sesuai kebutuhan seperti gambar berikut ini :



Gambar 2: Rancangan Layar Form Menu Utama

Flowchart Menu Utama menjelaskan alur proses saat kita berhasil *login* dan masuk ke dalam *Menu* Utama. Di dalam menu ini kita dapat memilih *menu* Pengguna dan memilih *menu* Keluar, kita juga bisa memilih *menu Email* untuk menampilkan *email* kotak masuk dan pesan terkirim, kita juga bisa memilih *menu*

Enkripsi yang mempunyai *submenu* Enkripsi Pesan, Enkripsi *File*, Dekripsi Pesan, Dekripsi *File*, dan *menu* Tentang yang mempunyai *submenu* Tentang Sistem dan Tentang Pembuat seperti gambar berikut ini :



Gambar 3: Flowchart Menu Utama

Algoritma berikut akan menjalaskan proses yang terjadi pada *Form Menu* Utama. Didalam *form* ini ada beberapa menu dan *sub menu* berikut ini adalah algoritma dari *Form Menu* Utama

1. Start
2. Tampil Menu Utama
3. Input Action
4. If action = Pengguna Then
7. Input Action
8. If action = "Keluar" Then
9. Kembali Ke Halaman Depan
10. Else
11. Kembali Ke Baris2
12. End if
13. Else if action = "*Email*" Then
14. Tampilkan Form List *Email* Masuk
15. Else if action = "Enkripsi" Then
16. Tampil semua menu enkripsi
17. Input action
18. If action = "Enkripsi Teks *Email*" Then
19. Tampil Form Enkripsi Teks *Email*
20. Else if action = "Enkripsi File *Email*" Then
21. Tampil Form Enkripsi File *Email*
22. Else if Action = "Dekripsi Teks *Email*" Then
23. Tampilkan Menu Dekripsi Teks *Email*
24. Else if Action = "Dekripsi File *Email*" Then
25. Tampilkan Menu Dekripsi File *Email*
26. Else if Action = "Tentang" Then
27. Tampilkan SubMenu Tentang
28. Else if Action = "Tentang Pembuat" Then
29. Tampilkan Form Pembuat Sistem
30. Else if Action = "Tentang Sistem" Then
31. Tampil Form Tentang Sistem
32. Else
33. Tampilkan Menu Utama
34. End if
35. Else
36. Kembali Ke Baris 2
37. End if
38. End if

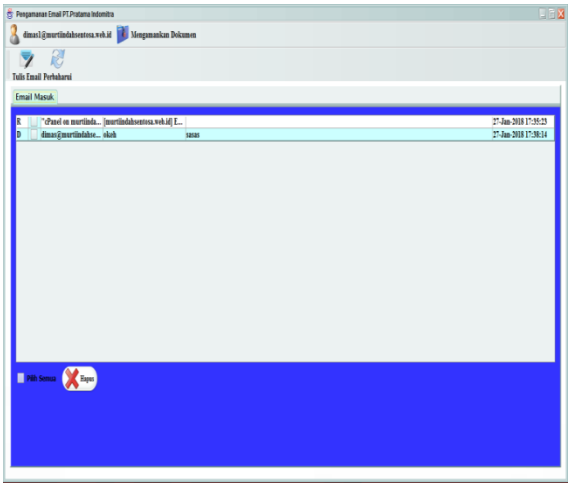
4. HASIL DAN PEMBAHASAN

Aplikasi pengamanan data melalui *email* dengan metode Eof Dan Rc4 untuk *file* yang berekstensi *.docx, .xlsx, pptx,*dan *.pdf* dapat berjalan dengan baik, termasuk spesifikasi tentang perangkat keras(*hardware*) dan perangkat lunak (*software*) yang digunakan. Serta beberapa pengujian yang berfungsi untuk mengevaluasi aplikasi ini agar mengetahui kelebihan dan kekurangan dari aplikasi ini.

4.1 Tampilan Layar Menu Utama

Tampilan layar dari menu utama ini muncul ketika pengguna berhasil masuk kedalam aplikasi ini. Pada menu ini terdiri dari beberapa *submenu* yang memiliki fungsi masing-masing, antara lain *Menu* Pengguna yang memiliki *submenu Logout*, *Menu Email* untuk menampilkan *List Email* Kotak Masuk dan Pesan Terkirim, *Menu* Enkripsi yang memiliki *submenu* Enkripsi Pesan,Enkripsi *File*, Dekripsi Pesan, Dekripsi

File, dan *Menu* Tentang yang memiliki *submenu* Tentang Sistem dan Tentang Pembuat. Tampilan *Form Menu* Utama dapat dilihat pada gambar berikut ini.



Gambar 4: Tampilan Layar Menu Utama

4.2 Tabel Pengujian

Didalam pengujian ini peneliti akan membahas perbandingan antara proses enkripsi dan dekripsi antara *file .docx, .xlsx, .pdf,* dan *.pptx.* Pengujiannya yaitu meliputi nama *file* asli, ukuran *file* asli, waktu proses enkripsi, nama *file* hasil enkripsi, ukuran hasil enkripsi, nama *file* setelah didekripsi, ukuran *file* hasil dekripsi dan waktu proses dekripsi.

Table 1: Hasil Proses Enkripsi Dan Dekripsi .docx

No.	Nama	Ukuran File (KB)	Waktu Proses (MiliSecond)		Ukuran File Setelah (KB)	
			Enkripsi	Dekripsi	Enkripsi	Dekripsi
1	Document_1	234	1.179881	0.878217	467	234
2	Document_2	21.926	6.456108	2.864384	43.850	21.926
3	Document_3	64	0.798785	0.728176	127	64
4	Document_4	16	0.245256	0.183629	31	16

a. Kelebihan Program

a. Aplikasi dapat digunakan dengan baik walaupun harus berjalan *online*.
b. Pengguna dapat meng-*embed* dan mengenkripsi *file* yang dilampirkan serta pengguna dapat mengenkripsi konten pesan sebelum dikirim.
c. Isi dari *file* dokumen *.docx, .xlsx, .pdf, .pptx,* yang sudah di *embed* tidak bisa di mengerti jika *file* tersebut dibuka oleh orang lain.
d. Jika *file embed* dibuka dengan aplikasi lain, isi *file* tidak akan terlihat seperti isi *file* yang sebenarnya, jadi isi *file* tetap terjaga kerahasiaanya.
e. *File* hasil *retrieve* tidak akan mengalami perubahan atau rusak.
f. Proses enkripsi dengan metode RC 4 dan *embed* memerlukan waktu rata-rata 7884,625 *millisecond*.
g. *File attachment* yang ada di pesan bisa langsung di *save* dan dapat di *retrieve* beserta dekripsi.

b. Kekurangan Program

a. Aplikasi ini hanya dapat melampirkan dan mengenkripsi *file* dokumen dengan format *.docx, .pdf, .pptx, .xlsx* saja.
b. Aplikasi ini hanya dapat memilih *file* gambar untuk disisipkan dengan *format .jpg, .png, .bmp* saja.
c. Ukuran *file* yang dikirim melalui layanan *email* di batasi hanya sampai 25mb.
d. Semakin besar ukuran *file* dokumen maka akan semakin lama waktu proses *embed* dan pengiriman pesan.
e. Aplikasi ini tidak dapat berjalan secara *offline*.
f. Proses pengiriman pesan *email* tergantung dengan koneksi internet.
g. Ukuran *file* yang telah di-*embed* dan enkripsi akan lebih besar dari ukuran *file* aslinya.

5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan terhadap permasalahan dari aplikasi yang telah dibuat, maka dapat ditarik kesimpulan dan saran yang mungkin diperlukan untuk pengembangan aplikasi ke tahap yang lebih baik kedepannya.

1. Kesimpulan

Dari proses pengujian dan pengerjaan yang peneliti buat, maka dapat disimpulkan beberapa hal, yaitu :

a. Algoritma kriptografi RC4 dan metode steganografi EOF dapat diimplementasikan pada aplikasi pengamanan dokumen melalui jalur *email*.

b. Dengan adanya program aplikasi kriptografi dan steganografi pengamanan dokumen, penyimpanan dan pertukaran informasi menjadi lebih aman.
c. Waktu yang digunakan untuk mengembed dan me-*retrievefile* berbanding lurus, jika ukuran *file* yang di proses semakin besar maka waktu yang digunakan semakin lama, sedangkan jika ukuran *file* yang di proses semakin kecil maka waktu yang digunakan semakin cepat.

2. Saran

Dari beberapa saran yang dapat disimpulkan dari peneliti, berikut saran yang dapat diberikan:

a. Penggunaan algoritma kriptografi RC4 dan metode steganografi EOF dalam mengembed dokumen diharapkan ukuran *file* bisa lebih kecil lagi setelah melewati proses embed dengan menggunakan kompresi.
b. Waktu proses diharapkan dapat lebih cepat dari yang sudah dihasilkan.
c. Menambah jumlah *file* yang dapat dienkripsi selain dengan tipe **.docx*, **xlsx*, **.pptx* dan **.pdf* saja.
d. Menambah format *file* penampung gambar selain dengan tipe *.jpg*, *.png*, *.bmp* saja.
e. Ukuran *file* yang akan disisipkan sebaiknya dapat lebih besar dari 200kb.
f. Algoritma enkripsi yang dibuat sebaiknya selalu ditingkatkan, karena dengan majunya perkembangan ilmu pengetahuan kriptografi yang pesat dan tidak dapat dipastikannya apakah algoritma ini masih bisa diandalkan.

6. DAFTAR PUSTAKA

Anti, U.A., Kridalaksana, A.H. & Khairina, D.M., 2017. STEGANOGRAFI PADA VIDEO MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN END OF FILE (EOF). Jurnal Informatika Mulawarman, 12(2), pp.104–111.

Aprisa & Monalisa, S., 2015. Rancang Bangun Sistem Informasi Monitoring Perkembangan Proyek Berbasis Web (Studi Kasus : Pt . Inti Pratama Semesta). Rekayasa dan Manajemen, 1(1), pp.49–54.

Ariyus, Dony. (2008). Ilmu Kriptografi (Teori,Analisis dan Implementasi). Yogyakarta.Andi Publlisher.

Embiring, S., 2013. MENYISIPKAN PESAN TEKS PADA GAMBAR DENGAN METODE END OF FILE. , 4(2), pp.45–51.

Hakim, E.L. & Utami, F.H., 2014. APLIKASI ENKRIPSI DAN DESKRIPSI DATA MENGGUNAKAN ALGORITMA RC4 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN PHP.
Media Informatika, 10(1), pp.1–7.

Haryanto, H., Wiryadinata, R. & Afif, M., 2014. Implementasi Kombinasi Algoritma Enkripsi Aes 128 Dan Algoritma Kompresi Shannon-Fano. Setrum, 3(1), pp.16–25.

Hasugian, A.H., 2013. Implementasi Algoritma Hill Cipher Dalam Penyandian Data. Pelita Informatika Budi Darma, IV(2), pp.115–122.

Nurhadian & Pudoli, A., 2016. Implementasi Keamanan File dengan Kompresi Huffman dan Kriptografi menggunakan Algoritma RC4 serta Steganografi menggunakan End of File Berbasis Desktop pada SMK Negeri 3 Kota Tangerang. Jurnal TICOM, 5(1), pp.39–46.

Nurmaesah, N., Lestari, T. & Mariana, A.R., 2017. APLIKASI STEGANOGRAFI UNTUK MENYISIPKAN PESAN DALAM MEDIA IMAGE. Jurnal TAM, 8(1), pp.13–17.

Perdana, W.P., Dwiono, W. & Harpawi, N., 2013. Pengontrolan Jarak Jauh Menggunakan Email Application. Teknik Elektro dan Komputer, I(I), pp.91–98.

Rijayana, I. et al., 2016. STEGANOGRAPHY MENGGUNAKAN METODE RC4. , (Selisik), pp.86–90.

Sadikin Rifki. 2012. Kriptografi Untuk Keamanan Jaringan. Yogyakarta.AndiPublisher

Setiawan, W., Juwairlah & Sofyan, H., 2012. Aplikasi Keamanan Pesan Menggunakan Algoritma Steganografi dan Kriptografi. Telematika, 8(2), pp.129–140.

Siswanto et al., 2016. PENGAMANAN DATA DENGAN MENGGUNAKAN ALGORITMA KRIPTOGRAFI AES , RC4 DAN KOMPRESI LZ77. , (Selisik), pp.115–120.

Sitorus, M., 2015. APLIKASI KEAMANAN DATA DENGAN TEKNIK STEGANOGRAFI MENGGUNAKAN METODE END OF FILE (EOF). , 1(1), pp.1–7.

Sumiaty, N. & Sumiaty, N., 2014. Literasi internet pada siswa sekolah menengah pertama. Penelitian Komunikasi, 17(88).

Wibowo, S.& S. et al., 2014. Aplikasi Enkripsi Email Dengan Menggunakan Metode Blowfish Berbasis J2Se. Techno.COM, 13(2), pp.75–83.

Hidayat, A.D. & Afrianto, I., 2017. Sistem Kriptografi Citra Digital Pada Jaringan Intranet Menggunakan Metode Kombinasi Chaos Map Dan Teknik Selektif. , IX(1),