IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL DAN STEGANOGRAFI END OF FILE (EOF) PADA APLIKASI PENGAMANAN EMAIL BERBASIS WEB PADA KANTOR KONSULTAN PAJAK HANDI

Esti Setiasih [1)], **M. Syafrullah** [2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : estisetiasih12@gmail.com[1)], mohammad.syafrullah@budiluhur.ac.id[2)]

Abstrak

Kantor Konsultan Pajak Handi merupakan jenis usaha yang bergerak dibidang jasa kepengurusan pajak. Dengan jumlah klien yang banyak, pertukaran data lebih aman dan cepat dengan menggunakan email. Data tersebut merupakan rahasia internal perusahaan sehingga tidak boleh diakses oleh pihak luar yang tidak memiliki kepentingan. Namun, kemajuan teknologi saat ini memungkinkan adanya penyadapan terhadap pesan yang dikirim melalui email. Oleh karena itu, untuk menjaga keamanan dan kerahasiaan data pada saat pengiriman dan penerimaan email dapat dilakukan dengan menerapkan teknik kriptografi dan teknik steganografi. Kriptografi merupakan ilmu untuk menjaga kerahasiaan informasi dengan melakukan penyandian terhadap data, sedangkan steganografi adalah ilmu dan seni yang digunakan untuk menyembunyikan pesan ke dalam suatu media sehingga pesan tersebut tidak diketahui keberadaanya. Media tersebut dapat berupa gambar, audio, atau video. Dalam penelitian ini, akan dibuat aplikasi yang dapat melakukan proses enkripsi dan dekripsi dengan mengkombinasikan algoritma kriptografi Elgamal dan steganografi End Of File (EOF). Algortima Elgamal merupakan contoh sistem kriptografi logaritma diskrit, dimana kunci yang digunakan untuk proses enkripsi berbeda dengan proses dekripsi (asimatris). Algoritma End Of File adalah salah satu teknik steganografi yaitu dengan menambahkan data dari pesan pada akhir file. Tapi pesan yang disisipkan ukurannya harus ditentukan agar tidak mempengaruhi ukuran atau citra penampung yaitu image (citra) tersebut. Elgamal digunakan untuk enkripsi teks pesan sedangkan End Of File digunakan untuk enkripsi lampiran pesan. Dengan adanya penggabungan algoritma ini diharapkan menghasilkan aplikasi yang baik untuk mengamankan proses pengiriman email. Sehingga tidak terjadi kekhawatiran pada saat pengiriman email ataupun membaca email. Akun yang digunakan untuk masuk ke aplikasi adalah akun gmail dimana akun tersebut wajib didaftarkan terlebih dahulu agar dapat login ke dalam aplikasi. Aplikasi dibuat dengan menggunakan bahasa pemrogaman PHP (Hypertext Preprocessor). Aplikasi ini diharapkan dapat membantu staff Kantor Konsultan Pajak Handi dan kliennya dalam proses pertukaran data.

Kata kunci: Kriptografi, Steganografi, Elgamal, End Of File

1. PENDAHULUAN

1.1. Latar Belakang

Kantor Konsultan Pajak Handi merupakan jenis usaha perorangan yang memberikan jasa layanan akuntansi, konsultasi manajemen, layanan perpajakan, konsultasi perpajakan, audit laporan perusahaan serta pelayanan-pelayanan lain yang berkaitan dengan perpajakan. Untuk membuat laporan perpajakan dibutuhkan data-data seperti data gaji karyawan, data pembelian barang, data penjualan barang, faktur pajak, data penyetoran modal, data hutang piutang dll. Data-data tersebut biasanya dikirim melalui email.

Keamanan data-data tersebut sangatlah penting karena data-data perpajakan berisi informasi yang bersifat rahasia sehingga tidak sembarangan orang berhak untuk mengetahuinya. Selain itu, kemajuan ilmu pengetahuan dan teknologi saat ini mendorong berkembangnya kejahatan teknologi komunikasi dan informasi lain seperti interupsi, modifikasi maupun fabrikasi. Hal inilah yang menuntut adanya pengamanan terhadap proses pengiriman data-data tersebut.

Untuk saat ini memang belum terjadi kasus pencurian data ketika berkomunikasi melalui email, tapi sebagai upaya pencegahan penggunaan aplikasi pengamanan email layak untuk diterapkan karena infomasi yang ada pada data tersebut sangatlah berharga. Informasi tersebut berhubungan dengan keuangan perusahaan. Karena kedepannya kejahatan teknologi akan semakin berkembang. Pada penulisan ini akan diimplementasikan teknik penggabungan kriptografi dan steganografi. Teknik kriptografi yang akan digunakan adalah Elgamal dan steganografi menggunakan metode End Of File (EOF).

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas maka rumusan masalah dalam perancangan aplikasi ini yaitu :

a. Bagaimana cara untuk mengamankan kerahasiaan informasi dari isi pesan dan file yang dilampirkan melalui email pada Kantor Konsultan Pajak Handi.
b. Bagaimana cara mengimplementasikan algoritma kriptografi Elgamal dan steganografi End Of File

(EOF) pada aplikasi pengaman email Kantor Konsultan Pajak Handi.

1.3. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah di atas, tujuan penulisan ini adalah :

a. Mengamankan informasi yang terdapat pada isi pesan dan lampiran yang dikirim atau diterima melalui email.
b. Mengembangkan suatu aplikasi keamanan email yang dapat melakukan enkripsi dan dekripsi terhadap isi pesan dan lampirannya dengan menggunakan kriptografi Elgamal dan steganografi End Of File (EOF) tanpa mengubah sedikitpun isi data.

1.4. Batasan Masalah

Agar tidak menyimpang dari pokok pembahasan, sehingga dalam menyelesaikan ini akan dibatasai pada beberapa hal berikut :

a. Metode algoritma kriptografi yang digunakan adalah Elgamal.
b. Metode algoritma steganografi yang digunakan adalah End Of File (EOF).
c. Data email yang diamankan adalah teks pesan dan file lampirannya yang berekstensi : *.docx, *.doc, *.xlsx, *.xls, dan *.pdf.
d. File gambar yang digunakan untuk menyisipkan berekstensi : *.jpg.
e. Ukuran maksimal file lampiran dibatasi maksimal sebesar 2 MB.
f. Aplikasi bahasa pemrograman yang digunakan yaitu bahasa pemrograman PHP (Hypertext Preprocessor).

2. LANDASAN TEORI

2.1. Definisi Kriptografi

Menurut Arius kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Arius, 2008).[1]

Sedangkan menurut Sadikin kriptografi awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern, kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern saja tidak berurusan hanya dengan penyembunyian pesan, namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi (Sadikin, 2012).[2]

2.2. Tujuan Kriptografi

Tujuan Kriptografi adalah sebagai berikut :

a. Confidentiality (kerahasiaan)
   Layanan yang ditujukan untuk menjaga pesan sehingga tidak dibaca pihak-pihak yang tidak memiliki kepentingan.
b. Authentication (Otentikasi)
   Layanan yang berhubungan dengan proses identifikasi kebenaran pihak-pihak yang saling berkomunikasi maupun identifikasi dari kebenaran sumber pesan.
c. Intengrity (Intengritas)
   Layanan yang menjamin bahwa pesan yang dikirimkan belum pernah dimanipulasi.
d. Nonrepudiaton
   Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan.

2.3. Metode Elgamal

Algoritma Elgamal dibuat oleh Taher Elgamal pada tahu 1984. Algoritma ini awalnya digunakan untuk proses digital signature, kemudian dimodifikasi sehingga bisa digunakan untuk proses enkripsi dan dekripsi. Menurut Munir keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit (Munir, 2004). [3]

Algoritma kunci publik elgamal merupakan algoritma blok chiper yaitu algoritma yang melakukan proses enkripsi pada blok-blok plaintext yang kemudian menghasilkan blok-blok chipertext, yang nantinya blok-blok chipertext tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi plaintext semula.

Kelebihan dari algoritma ini terletak pada proses pembuatan kunci yang menggunakan logaritma diskrit dan juga proses enkripsi yang menghasilkan data yang ukurannya dua kali lebih besar dari data sebelum dienkripsi. Kekurangan dari algoritma ini yaitu diperlukan sumberdaya yang besar karena chipertext yang dihasilkan dua kali panjang plaintext serta diperlukan processor yang dapat melakukan komputasi untuk perhitungan logaritma perpangkatan besar.

Berikut besaran-besaran yang digunakan di dalam algoritma Elgamal :

1) Bilangan prima, p (bersifat rahasia)
2) Bilangan acak, g (g < p) (bersifat tidak rahasia)
3) Bilangan acak, x (x < p) (bersifat rahasia)
4) M (plaintext) (bersifat rahasia)
5) a dan b (chipertext) (bersifat tidak rahasia)

Proses pembangkitan kunci merupakan proses menentukan suatu bilangan yang akan digunakan sebagai kunci untuk mengenkripsi dan mendekrip pesan. Kunci untuk enkripsi dibangkitkan dari nilai p, g, y sedangkan untuk kunci dekripsi terdiri dari nilai x, p. Berikut adalah langkah-langkah dalam pembuatannya :

1) p merupakan bilangan prima dengan ketentuan p > 255
2) g adalah bilangan acak dengan ketentuan g < p
3) x adalah bilangan acak x dengan ketentuan $1 \leq x \leq p - 2$
4) Hitung nilai y dengan rumus $y = g.x \bmod p$

Kunci publiknya adalah y, g, p sedangkan kunci privatenya adalah x.

a. Proses Enkripsi Algoritma Elgamal

Berikut adalah langkah-langkah enkripsinya :

1) Plaintext disusun menjadi blok-blok m1, m2,..., nilai setiap blok di dalam selang [0, p – 1]
2) Ubah nilai dari blok pesan ke dalam nilai kode ASCII
3) Pilih bilangan acak k, dengan ketentuan $1 \leq k \leq p - 1$ sebanyak m
4) Setiap blok m dienkripsi menggunakan rumus :
   Gamm (a) = gki mod p
   Delta (b) = yki.m mod p
5) Susun chipertext dengan urutan a1, b1, a2, b2, a3, b3, ..., ...,

a dan b adalah pasangan chipertext yang dihasilkan dari proses enkripsi untuk blok pesan m.

b. Proses Dekripsi Algoritma Elgamal

Berikut adalah langkah-langkah dekripsinya :

1) mi = bi.ai^p-1-x mod p
2) nilai mi yang didapat dalam bentuk ASCII kemudian diubah menjadi plaintext
3) Susun plaintext dengan urutan m1, m2, m3, ..., mn

m merupakan pesan asli (plaintext) yang dihasilkan dari proses dekrip dari nilai chipertext a dan b.

2.4. Steganografi

Steganografi berasal dari bahasa Yunani yaitu dari kata stegos yang artinya penyamaran dan kata graphia yang berarti tulisan. Menurut Munir steganografi merupakan teknik yang digunakan untuk menyembunyikan informasi rahasia ke dalam suatu media agar keberadaan dari informasi rahasia tersebut tidak diketahui oleh orang lain (Munir, 2004). [4]

Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Media yang telah disisipi data disebut stegomessage. Proses penyembunyian pesan rahasia ke dalam media disebut penyisipan (embedding), sedangkan proses sebaliknya disebut ekstrasi. Penambahan kunci yang bersifat opsional dimaksudkan untuk meningkatkan keamanan (Alatas, 2009). [3]

2.5. Metode End Of File

Metode End Of File merupakan salah satu metode yang digunakan untuk steganografi. Teknik ini digunakan dengan cara menambahkan pesan rahasia pada akhir file. Besar ukuran file gambar yang telah disisipkan data sama dengan ukuran file gambar sebelum disisipkan data ditambah dengan ukuran dari data rahasia yang telah diubah menjadi encoding file.

Metode EOF tidak akan mengubah isi awal dari file yang disisipi. Sebagai contoh, jika akan menyisipkan sebuah pesan kedalam sebuah file dokumen, isi dari dokumen tersebut tidak akan berubah. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan metode steganografi yang lain. Karena disisipkan pada akhir file, pesan yang disisipkan tidak akan bersinggungan dengan isi file, hal ini menyebabkan integritas data dari file yang disisipi tetap dapat terjaga. Namun, metode EOF akan mengubah besar ukuran file sesuai dengan ukuran pesan yang disisipkan kedalam file awal namun tidak mengubah citra daripada media yang dipakai sebagai tempat penyisipan pesan tersebut.

a. End Of File untuk Proses Embed

Proses embedding atau penyisipan pesan menggunakan metode End Of File adalah sebagai berikut :

1) Input Ciphertext yang akan disisipkan.
2) Input Citra yang akan menjadi media penyisipan ciphertext (cover image).
3) Baca nilai setiap pixel citra.
4) Tambahkan ciphertext sebagai nilai akhir pixel citra dengan diberi karakter penanda sebagai penanda akhir ciphertext.
5) Petakan menjadi citra baru. (Wandani dkk, 2012), [5]

b. End Of File untuk Proses Retrieve

Proses extraction atau pengambilan ciphertext dari media menggunakan metode End Of File adalah sebagai berikut :

1) Input citra yang telah disisipkan ciphertext (stego image)
2) Baca nilai pixel stego image yang terdapat padabaris terakhir matriks pixel citra.
3) Ambil ciphertext yang terdapat pada stego image, yaitu nilai pixel awal yang terdapat pada baris terakhir matriks pixel citra sampai nilai decimal karakter penanda. (Wandani dkk, 2012)

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Rancangan Program

User mendaftarkan akun gmailnya pada aplikasi. Kemudian pada form daftar user mendapatkan 2 kunci yaitu kunci publik dan kunci private. Pada saat akan mengenkripsi pesan, user menggunakan kunci publik milik penerima pesan sehingga pesan asli (plaintext) yang dikirimkan berubah menjadi chipertext. Kemudian untuk lampiran akan diembed ke dalam sebuah gambar.

User yang menerima pesan berupa chipertext dapat mengembalikan pesan tersebut ke bentuk plaintext dengan menggunakan kunci private. Untuk mengembalikan file yang sudah diembed menjadi file asli, user dapat memilih form buka file. Namun, sebelumnya user harus melakukan verifikasi terlebih dahulu.

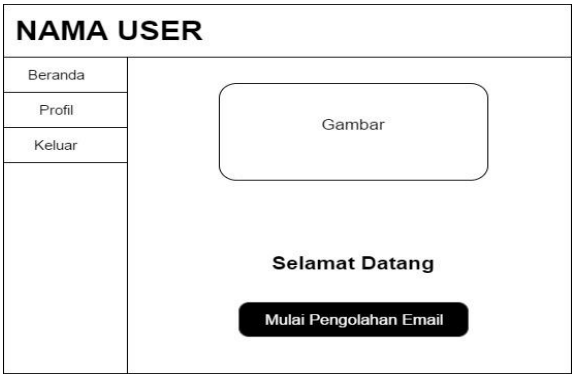
3.2. Skema Proses Aplikasi

Aplikasi ini menggunakan teknik kriptografi Elgamal untuk mengenkripsi isi pesan dan steganografi End Of File (EOF) untuk menyembunyikan file lampiran ke dalam sebuah gambar. Alur dari aplikasi ini akan dijabarkan sebagai berikut:

a. Pertama user pengirim dan user penerima harus mendaftarkan akun gmailnya pada aplikasi.
b. Setelah pendaftaran sukses, kemudian user login dengan memasukkan alamat email dan password.
c. Setelah proses login berhasil maka akan muncul menu beranda, kemudian user pengirim pilih menu Mulai Pengolahan Email lalu pilih menu Tulis Pesan.
d. Lalu user pengirim memasukkan alamat email penerima, subjek email dan menuliskan teks pesan.
e. Teks pesan dapat dienkripsi dengan memilih kunci publik milik user penerima.
f. Setelah itu pilih jenis file yang akan disisipkan ke dalam sebuah gambar lalu kirim pesan.
g. User penerima akan menerima teks pesan serta file yang sudah terenkripsi.
h. User penerima login ke aplikasi.
i. Untuk membuka pesan email yang dienkripsi, user harus melakukan verifikasi (input password login) untuk dapat mendekrip teks pesan kemudian pilih buka pesan sedangkan untuk file yang diembed ke gambar harus di unduh sebelum di dekrip.
j. Untuk mendekrip file yang sudah diunduh pilih menu Buka File, user penerima melakukan verifikasi sebelum mendekrip file, lalu akan muncul file asli. Untuk mengetahui isi file tersebut harus diunduh terlebih dahulu.
k. Jika user penerima ingin keluar, pilih menu Keluar. Namun jika ingin membalas pesan tersebut, user dapat mengulangi langkah A.

3.3. Rancangan Layar Form Beranda

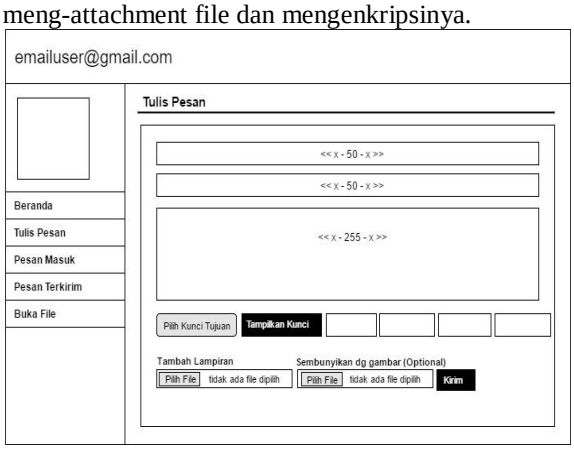
Setelah login berhasil, user masuk ke dalam form beranda kemudian pilih menu Pengolahan Email maka akan muncul daftar menu dari aplikasi ini. Menu tulis pesan untuk menuliskan pesan baru, menu pesan masuk untuk melihat daftar pesan yang diterima, dan menu buka file untuk mendekrip file yang diembed ke gambar. Seperti pada gambar 1 berikut ini :



Gambar 1 : Rancangan Layar Form Beranda

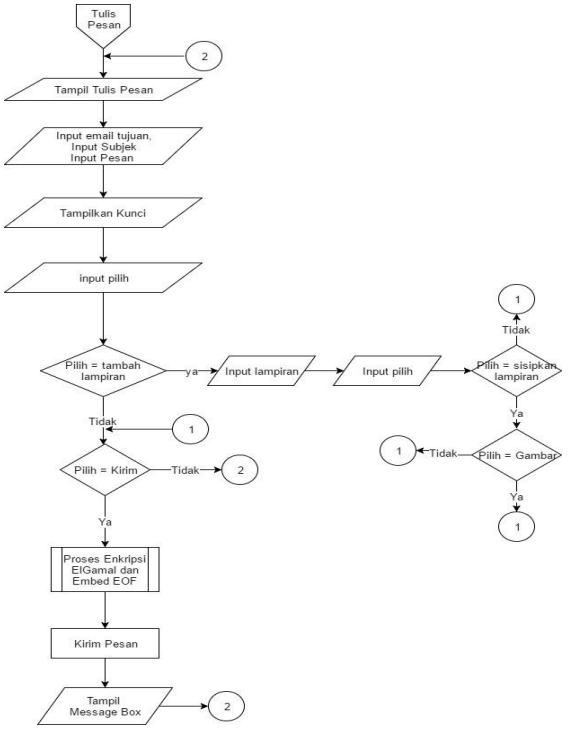
3.4. Rancangan Layar dan Flowchart Tulis Pesan

Menu tulis pesan digunakan untuk menulis pesan baru, user diharuskan menginputkan alamat email tujuan, subjek, dan isi dari pesan. User juga bisa meng-attachment file dan mengenkripsinya.



Gambar 2 : Rancangan Layar Form Tulis Pesan

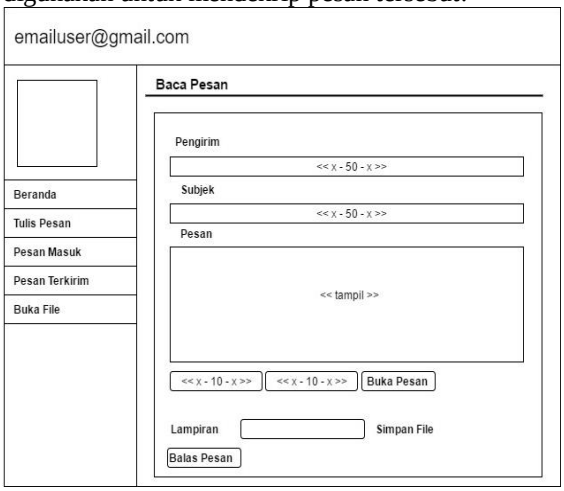
Flowchart Tulis Pesan ini menjelaskan tentang alur yang *user* lakukan untuk mengenkripsi dan melakukan steganografi terhadap pesan yang ingin *user* kirimkan.



Gambar 3 : Flowchart Tulis Pesan

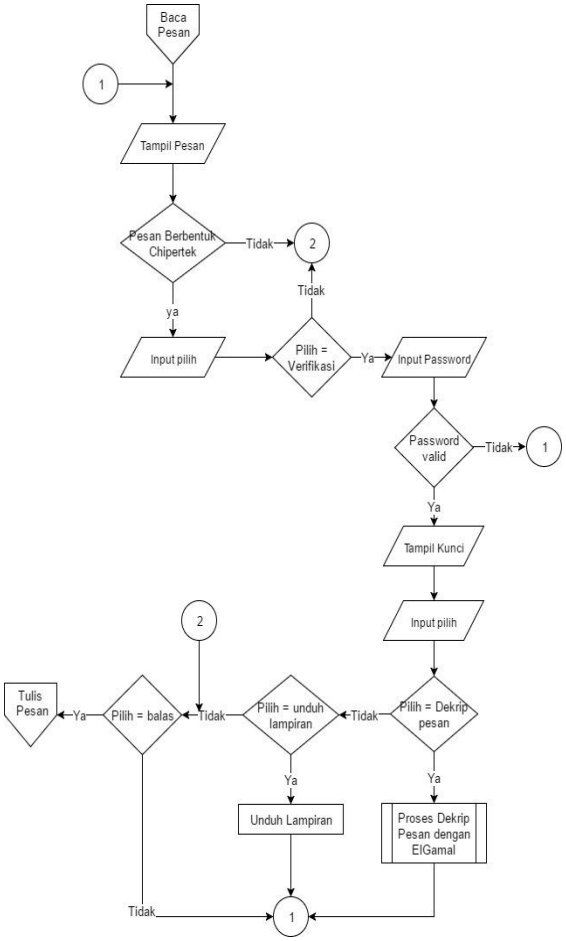
3.5. Rancangan Layar dan Flowchart Baca Pesan

User dapat membaca pesan yang berbentuk chipertext setelah melakukan verifikasi sehingga aplikasi akan mmunculkan dua kunci privat yang digunakan untuk mendekrip pesan tersebut.



Gambar 4: Rancangan Layar Form Baca Pesan

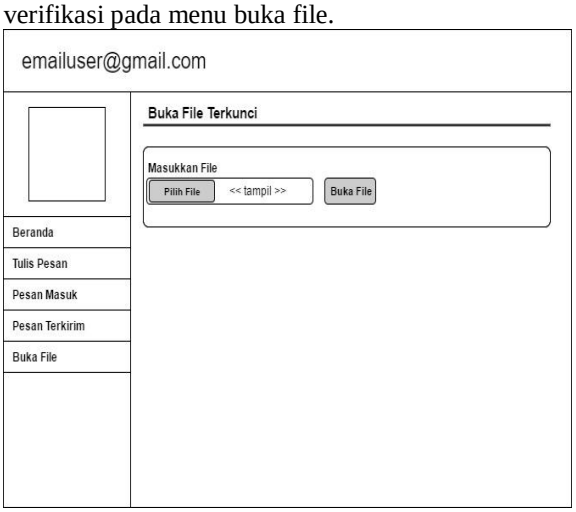
Flowchart Baca Pesan Menjelaskan alur yang dilakukan user untuk membaca pesan yang diterima yang berbentuk plaintext ataupun chipertext.



Gambar 5 : Flowchart Tulis Pesan

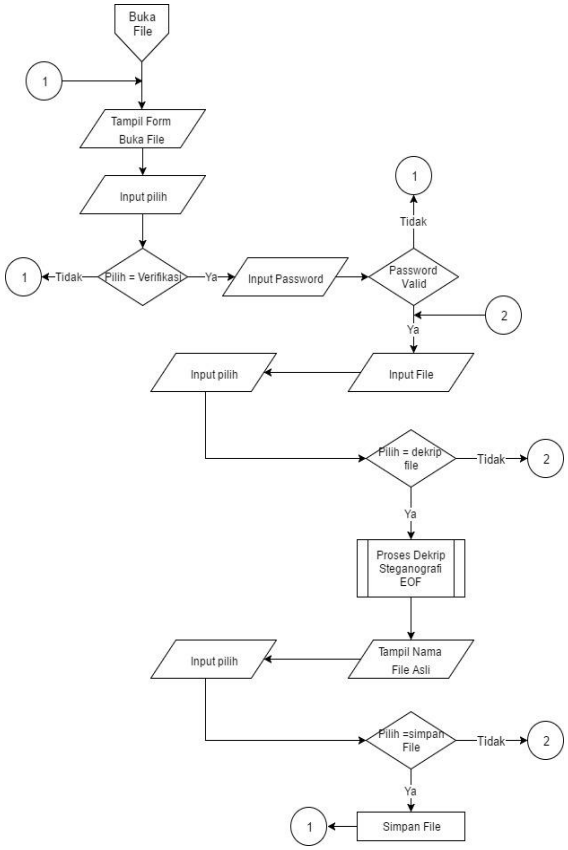
3.6. Rancangan Layar Dan Flowchart Dekrip File

User dapat mendekrip file setelah melakukan verifikasi pada menu buka file.



Gambar 6: Rancangan Layar Form Buka File

Berikut Flowchart dari form Buka File. *Flowchart* ini menjelaskan alur proses untuk mendekrip file .



Gambar 7 : Flowchart Buka File

4. HASIL DAN PEMBAHASAN

4.1. Spesifikasi Hardware dan Software yang dibutukan

Pengimplementasian aplikasi ini memerlukan 1 set komputer / notebook (hardware) dan beberapa software pendukung.

a. Spesifikasi Perangkat keras (Hardware)

Perangkat keras yang digunakan untuk menjalankan aplikasi ini secara maksimal adalah sebagai berikut :

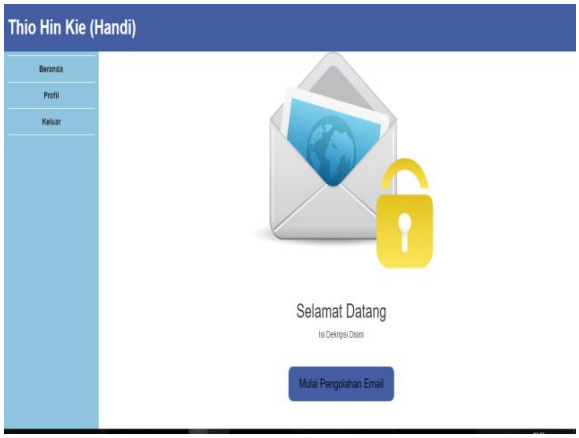
1) Processor Intel Core i3-3217U CPU @ 1.80 GHz
2) RAM / Memory 2 GB
3) Hardisk 300 GB

b. Spesifikasi Perangkat Lunak (Software)

1) Sistem Operasi Microsoft Windows 10
2) PHP 5.6, Mysql dan XAMPP
3) Browser (Google Chrome)

4.2. Tampilan Layar Form Beranda

Tampilan layar dari form home bisa dilihat dari gambar 8.



Gambar 8 : Tampilan Layar Form Beranda

Setelah user memilih menu Mulai Pengolahan Email maka user akan diarahkan ke menu pesan masuk. Pada form ini terdapat beberapa menu yang dapat digunakan oleh user yaitu menu Tulis Pesan, Pesan Masuk, Pesan Keluar, Dekrip File, Profil dan keluar

Gambar 9 : Tampilan Layar Form Pesan Masuk

4.3. Tabel Pengujian

Dalam pengujian kali ini, akan dibahas perbandingan antara proses embed dan retrieve. Lebih detailnya akan di sajikan dalam tabel berikut ini :

Tabel 1 : Tabel Hasil Embed

Nama Gambar	Nama Lampiran	Size Gambar	Size lampiran	Nama Hasil Embed	Ukuran Hasil Embed
spons.jpg	surat.docx	15 KB	13 KB	en_spons.png	88 KB
Sukarno.jpg	Perjanjian_sewa.doc	178 KB	59 KB	en_sukarno.png	225 KB
Hallo.jpg	faktur.pdf	85 KB	46 KB	en_hallo.png	361 KB

Tabel 2 : Tabel Hasil Retrieve

Nama Gambar	Size gambar	Nama Hasil Retrieve	Hasil Retrieve
en_spons .png	88 KB	de_surat.docx	13 KB
en_sukar no.png	225 KB	de_perjanjian_s ewa.doc	59 KB
en_hallo. png	361 KB	de_faktur.pdf	46 KB

4.4. Evaluasi Program

Aplikasi kriptografi dan steganografi dengan menggunakan algoritma ElGamal dan EOF dapat diimplementasikan dengan baik. *File* yang dapat di *upload* dibatasi, maksimal 2 MB. Hal ini dilakukan agar *user* tidak terlalu lama saat proses *upload* maupun *download*. Gambar yang bisa disisipi juga hanya yang berkekstensi .*jpg. Setelah dilakukan analisa dari hasil pengujian aplikasi, akan dijelaskan tentang hasil evaluasi, kelebihan, dan kekurangan dari aplikasi ini, yaitu sebagai berikut :

a. Kelebihan Aplikasi

1) Dapat digunakan dengan mudah, karena tampilan yang dirancang *user- friendly*.
2) *File* yang dikirim akan aman karena sudah di enkripsi.
3) Isi dan format file dari hasil enkripsi, tidak mengalami perubahan sedikit pun.
4) Proses enkripsi dan dekrip menggunakan kunci yang berbeda sehingga tidak muncul masalah cara pendistribusian kunci.

b. Kekurangan Aplikasi

1) *File* yang diupload maksimal 2 MB saja.
2) File yang dapat dilampirkan terbatas yaitu 1 file saja.
3) Penerima *email* tidak bisa melihat *file* yang disisipkan sebelum melakukan dekrip gambar.
4) Waktu yang dibutuhkan untuk melakukan proses enkripsi pada file yang memiliki ukuran besar masih kurang cepat.
5) Apabila daftar pesan yang ada di pesan masuk dan pesan terkirim banyak, dibutuhkan waktu yang lebih lama untuk menampilkan pesan.
6) Aplikasi tidak dapat digunakan di *smartphone*.

5. KESIMPULAN

Berdasarkan hasil analisa yang dimulai dari proses pengumpulan informasi, perumusan masalah, pemecahan masalah serta proses pengembangan aplikasi ini, didapatkan beberapa kesimpulan dan saran sebagai berikut :

5.1. Kesimpulan

Berdasarkan hasil analisa pada bab-bab sebelumnya, dapat disimpulkan bahwa aplikasi untuk pengamanan *email* menggunakan algoritma ElGamal dan EOF sangat diperlukan karena :

a. Sebuah aplikasi yang mengimplementasikan algoritma kriptografi ElGamal dan steganografi EOF untuk keamanan data pada saat pengiriman *email* telah diciptakan.
b. Dengan adanya program aplikasi kriptografi dan steganografi, proses pertukaran data atau *file* melalui *email* menjadi lebih aman.

File yang disisipkan ke dalam gambar tidak mengalami perubahan isi sedikitpun

5.2. Saran

Terbatasnya waktu yang diberikan untuk menyelesaikan penulisan ini menyebabkan penyelesaian permasalahan yang telah dikembangkan masih jauh dari sempurna. Oleh karena itu, diperlukan saran untuk pengembangan aplikasi lebih lanjut antara lain :

a. Gambar yang disisipkan bukan hanya format *.jpg / *.jpeg namun juga *.png.
b. File yang dapat dilampirkan hanya satu file saja, untuk pengembangannya penulis berharap file berekstensi zip dapat dilampirkan juga, sehingga user dapat mengirim beberapa pesan sekaligus dalam satu folder.
c. Untuk kedepannya akun yang dapat menggunakan aplikasi ini tidak hanya akun *gmail* saja.
d. Untuk kedepannya penulis berharap aplikasi ini dapat dikembangkan untuk *smartphone.*

6. DAFTAR PUSTAKA

[1] Ariyus, Doni, 2008, Pengantar Ilmu Kriptografi, Yogyakarta, ANDI

[2] H. Wandani, M. Andri Budiman, A. Sharif, 2015, Implementasi Sistem Keamanan Data Dengan Menggunakan Teknik Steganografi End Of File dan Rabin Public Key Cryptosystem

[3] Putri, Alatas, 2009, Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital, Jakarta, Universitas Gunadarma

[4] R. Munir, 2006, Kriptografi, Bandung, Informatika Bandung

[5] Sadikin, Rifki, 2012, Kriptografi Untuk Keamanan Jaringan, Yogyakarta, ANDI