Implementasi Kriptografi Dengan Algoritma Base64 Dan Advance Encryption Standard Untuk Mengamankan Data Email Berbasis Web

Dimas Bayu Nurcahyo[1)], Safrina Amini[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : dimasbayu06@gmail.com[1)], safrina.amini@budiluhur.ac.id[2)]

ABSTRAK **dimasbayu06@gmail.com**

Hingga saat ini teknologi informasi berkembang dengan cepat, sehingga semua orang dapat bertukar informasi melalui media komunikasi apapun. Pengiriman atau pertukaran data merupakan hal yang selalu terjadi dalam dunia teknologi informasi, salah satu aplikasi yang banyak digunakan adalah adalah email. PT. Semanta Mulia Transport adalah perusahaan swasta yang bergerak dibidang jasa transportasi yang mempunyai banyak rekanan bisnis maupun pelanggan dipulau jawa maupun diluar pulau jawa. Sehingga dilakukan transaksi elektronik menggunakan email untuk pengiriman surat penawaran bus, invoice tagihan sewa bus, gaji karyawan dan file lainnya yang harus dilindungi agar terhindar dari pencurian dan penyalahgunaan dari file-file tersebut, serta untuk menghindari terjadinya akses terhadap file-file tersebut dari pihak yang tidak berkepentingan. Untuk meminimalisasi serangan terhadap transmisi data, dapat dilakukan dengan menggunakan teknik kriptografi. Penelitian ini bertujuan untuk membuat aplikasi pengamanan email pada pesan email dan file attachment-nya dengan mengimplementasikan algoritma kriptografi base64 dan Advanced Encryption Standard-128. Dengan aplikasi ini, keamanan dalam mengirim dan menerima email dapat terjamin. Walaupun pesan email bisa diambil orang lain tetapi mereka tetap tidak akan bisa membacanya karena teks tertampil dalam dengan kata-kata acak dan tidak beraturan yang sulit di mengerti. Sehingga dapat mengambil kesimpulan bahwa aplikasi ini dapat membuat email menjadi lebih aman.

Kata kunci : Kriptografi, *Base*64*, Advanced Encryption Standard*, Enkripsi, Dekripsi, *Email*

1. PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi komunikasi saat ini telah berjalan dengan sangat pesat, sehingga memudahkan setiap orang untuk mendapatkan informasi dengan cepat. Hampir semua lapisan masyarakat tidak bisa lepas dari teknologi, Sehingga banyak sekali data yang disimpan dan dikirim dengan menggunakan teknologi. Salah satu aplikasi yang banyak digunakan adalah surat elektronik atau *email*. Karena banyaknya pengguna *email* yang tidak menggunakan komputer atau laptop milik pribadi, terutama karyawan disuatu perusahaan. Sehingga, informasi pesan yang dikirimkan sangat rentan akan pembajakan informasi pesan yang sifatnya sangat rahasia atau penting yang tidak boleh di ketahui orang lain. PT. Semanta Mulia Transportasi adalah salah satu perusahaan swasta yang bergerak dibidang jasa transportasi. Jumlah karyawan tetap di PT. Semanta Mulia Transport memang tidak terlalu banyak, namun mempunyai banyak rekanan bisnis maupun pelanggan dipulau jawa maupun diluar pulau jawa. Sehingga dilakukan transaksi elektronik menggunakan *email* untuk pengiriman surat penawaran *bus*, *invoice* tagihan sewa *bus*, gaji karyawan dan *file* lainnya. Kemudahan pengaksesan itulah yang menyebabkan masalah keamanan sangatlah penting dalam sebuah sistem informasi. Jatuhnya data atau informasi ke pihak yang tidak berhak untuk mengakses data akan menyebabkan kerugian, karena data tersebut dapat dimanipulasi, dirusak, atau disalahgunakan oleh pihak-pihak yang tidak mempunyai wewenang.

Berdasarkan uraian di atas, maka dibuat suatu sistem pengamanan informasi baik saat pengiriman maupun penerimaan *email*. Keamanan aplikasi ini sangat terjaga karena menggunakan algoritma *Base*64 dan algoritma *Advance Encryption Standard*-128. Dengan aplikasi ini, keamanan dalam mengirim dan menerima *email* dapat terjamin. Meskipun pesan *email* dapat diambil orang lain tetapi mereka tetap tidak akan bisa membacanya karena data tertampil dalam dengan kata-kata acak dan tidak beraturan yang sulit di mengerti. Sehingga apabila orang lain melihat isi dari data *email* tersebut akan mengalami kesulitan.

1.2. Tujuan Penelitian

Tujuan penilitian berdasarkan rumusan masalah sebagai berikut :

a. Mengembangkan suatu aplikasi kemanan yang dapat mengamankan data dan informasi pelanggan yang dikirim atau diterima melalui media *email*.
b. Menggunakan algoritma *base*64 dan *Advanced Encryption Standard* – 128 untuk mengenkripsi

data dan informasi yang dikirim atau di terima melalui media *email*.

1.3. Batasan masalah

Batasan masalah dari pembuatan aplikasi ini adalah sebagai berikut :

a. Metode algoritma kriptografi yang digunakan adalah *base*64 dan *Advanced Encryption Standar*d–128.
b. Data yang dienkripsi dan dideskripsi adalah data berbentuk teks dan file attachment.
c. Bahasa pemograman yang digunakan adalah PHP.
d. *Setting* IMAP pada GMail, Yahoo dan Outlook *Mail* harus diaktifkan terlebih dahulu sebelum menjalankan aplikasi ini.
e. Aplikasi yang dibuat berbasis web, dijalankan dengan menggunakan *browser*.
f. Aplikasi tidak bisa digunakan saat *offline*.

2. LANDASAN TEORI

2.1 Definisi *Email*

Electronic-Mail (*Email*) merupakan fasilitas untuk saling berkomunikasi. Untuk mengirim sebuah informasi data dari suatu pihak ke pihak lain dengan berdasarkan sebuah penamaan atau alamat *e-mail* yang akan dituju [1].

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti (tulisan). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan / data ketika dikirim dari suatu tempat ke tempat yang lain [2]. Kriptografi adalah keterampilan yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti keabsahan data, integritas data, serta autentifikasi data. Sistem kriptografi adalah suatu fasilitas untuk mengkonversikan pesan jelas (*plaintext*) ke pesan yang telah disandikan (*ciphertext*). Proses konversi ini disebut enkripsi (*encryption*). Sebaliknya, menerjemahkan cipherteks menjadi plainteks disebut dengan dekripsi (*decryption*). Proses enkripsi dan dekripsi menggunakan satu atau beberapa kunci kriptografi [3].

2.2 Algoritma Kriptografi *Base*64

Transformasi *base*64 merupakan salah satu algoritma untuk *encoding* dan *decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64. Karakter yang dihasilkan pada transformasi base64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambah simbol "+" dan "/" serta satu buah karakter sama dengan (=) di dua karakter terakhir yang dipakai untuk pengisian pad atau dengan kata lain penyesuaian dan menggenapkan data binary. Prinsip *encoding*-nya adalah untuk melakukan *obfuscation* atau pengacakan data [4].

2.3 Algoritma *Advanced Encryption Standard*-128

AES (*Advanced Encryption Standard*) [nis01] adalah teknik enkripsi yang dijadikan *standard* FIPS oleh NIST tahun 2001. AES dimaksudkan akan, secara bertahap, menggantikan DES sebagai *standard* enkripsi di Amerika Serikat untuk abad ke 21. (DES sebagai *standard* FIPS telah dicabut, Mei 2005) [5].

Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi (bersifat simetri), serta masukkan dan keluaran data berupa blok dengan urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut sebagai blok data atau plainteks yang nantinya akan dienkripsi menjadi *chipertext*. *Cipher key* dari AES terdiri dari *key* dengan panjang 128 *bit*, 192 *bit*, atau 256 *bit*. Perbedaan panjang kunci akan mempengaruhi jumlah round (putaran) yang akan diimplementasikan pada algoritma AES ini. Ada 10, 12, atau 14 putaran dalam AES yang sesuai dengan ukuran kunci yang digunakan. Setiap putaran mengandung:

a. Penggantian Byte yang sama dengan DES.
b. Peralihan = pertukaran baris.
c. Campur Jalur = peralihan kiri dan XOR bit-bit.
d. Penambahan sub-kunci = XOR bagian kunci dengan keputusan kitaran [6].

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Analisa Masalah

Saat ini internet sering digunakan oleh manusia untuk mengirim pesan atau informasi dengan menggunakan fasilitas *email*, baik *email* pribadi ataupun *email* yang diberikan dari perusahaan. Sebagian orang banyak yang menganggap bahwa informasi yang dikirimkan melalui *email* sangat aman. Tanggapan itu tidak sepenuhnya salah, semakin berkembangnya teknologi dan berharganya informasi tersebut maka semakin banyak orang yang menjadi target serangan oleh pihak yang tidak bertanggung jawab. Karena pada dasarnya proses pengiriman *email* hanya melakukan pengiriman pesan tanpa melakukan pengamanan apapun terhadap pesan yang dikirim.

Bertukar pesan bagi PT. Semanta Mulia Transportasi sangat penting karena rata-rata pesan yang dikirim berupa surat penawaran bus, invoice tagihan sewa bus. Oleh karena itu diperlukan aplikasi pengirim email yang dapat mengamankan isi pesan atau informasi yang ada didalamnya.

3.2 Penyelesaian Masalah

Berdasarkan permasalahan yang diuraikan diatas, maka dibutuhkan aplikasi pengirim *email* yang dapat mengamankan isi pesan atau informasi yang ada didalamnya. Untuk membuat aplikasi tersebut, digunakan teknik yang disebut kriptografi. Proses enkripsi berfungsi untuk mengubah pesan *email* yang berisi *plaintext* atau teks biasa menjadi *ciphertext* atau teks acak yang tak terbaca. Sebaliknya, menerjemahkan *ciphertext* menjadi *plaintext* disebut dengan dekripsi. Proses enkripsi dan dekripsi menggunakan satu atau beberapa kunci kriptografi. Maka dengan penerapan kriptografi ini kita dapat mencegah suatu pesan dan data yang bersifat rahasia itu dicuri, dilihat ataupun dimengerti oleh pihak yang bukan wewenangnya.

Aplikasi kriptografi yang dibuat menggunakan algorima *Base*64 algoritma *Advance Encryption Standard* 128-bit. Algorima *Base*64 adalah skema *encoding* yang merepresentasikan data biner ke dalam format ASCII. Algoritma *Advance Encryption Standard* 128-bit yang bersifat algoritma kriptografi simetris, jadi kunci yang digunakan saat enkripsi dan dekripsi sama.

3.2 Skema Proses Sistem Aplikasi

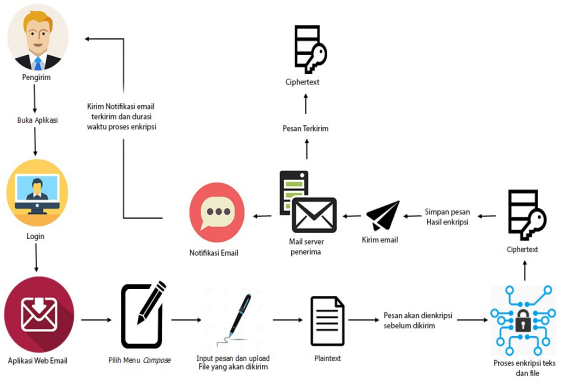
Untuk Menyelesaikan masalah diatas, maka diuraikan skema proses aplikasi. Berikut adalah tahapan-tahapan dalam pengiriman *email*.

a. Proses Pengiriman *Email*

Berikut adalah tahapan pada proses pengiriman *email* :

a) Langkah pertama untuk menggunakan aplikasi ini adalah pengirim membuka aplikasi pada *browser*.
b) Pengiriman melakukan *login* dengan *username* dan *password* dengan *email* pengirim (Gmail, Yahoo dan Outlook).
c) Jika pengirim baru pertama kali mengakses aplikasi ini, saat login tidak langsung bisa masuk ke aplikasi ini. Pengirim akan mendapatkan *email* yang berisikan konfirmasi bahwa penerima akan *login email* melalui aplikasi ini dan pastikan IMAP pada akun *email* sudah aktif.
d) Setelah *Login* berhasil dan masuk ke dalam *Form Home* aplikasi, pengirim memilih menu *compose* untuk melakukan pengiriman pesan.
e) Pengirim meng-*input* alamat *email* penerima, *subject,* isi pesan serta melampirkan *file* jika diperlukan sebelum melakukan pengiriman *email*.
f) Pada proses pengiriman, sistem yang ada diaplikasi akan melakukan proses enkripsi terlebih dahulu.
g) *Plaintext* yang didapat lalu diubah oleh sistem menjadi *ciphertext* dengan menggunakan *subject* sebagai kuncinya, karena itu *subject* harus diisi dan kemudian pesan tersebut dikirim ke *email* tujuan.
h) Aplikasi akan mengirim pesan yang telah tersimpan di *mail server* pengirim ke alamat *email* penerima.
i) *Mail server* pengirim akan menyimpan pesan berbentuk *ciphertext* yang telah dikirimkan oleh pengirim.
j) Pengirim akan mendapatkan notifikasi pesan telah terkirim dan durasi waktu proses enkripsi.

Berikut ini adalah gambaran alur kerja aplikasi untuk proses pengiriman *email* :



Gambar 1: Alur Proses Pengiriman Email

b. Proses Penerimaan *Email*

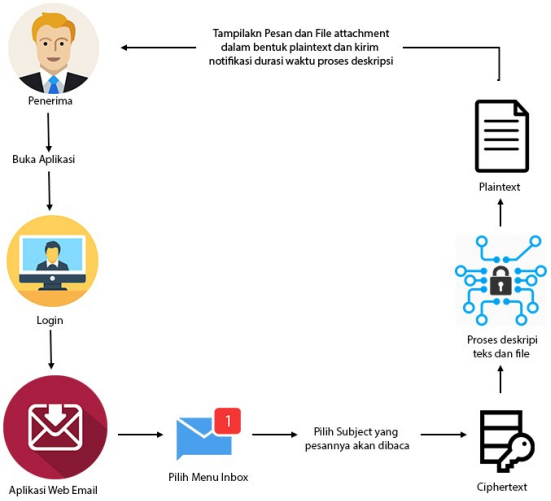
Berikut adalah tahapan pada proses penerimaan *email* :

a) Pertama-pertama pengirim membuka aplikasi pada *browser* untuk membuka aplikasi.
b) Pengiriman melakukan *login* dengan *username* dan *password* dengan *email* pengirim (Yahoo dan Outlook).
c) Jika penerima baru pertama kali mengakses aplikasi ini, saat *login* tidak langsung bisa masuk ke aplikasi ini. Penerima akan mendapatkan email yang berisikan konfirmasi bahwa penerima akan login email melalui aplikasi ini dan pastikan IMAP pada akun *email* sudah aktif.
d) Setelah *Login* berhasil dan masuk ke dalam *Form Home* aplikasi, pengirim memilih menu *inbox,* lalu muncul tampilan *list view inbox*. Untuk membuka pesan yang

terenkripsi, penerima mengklik *subject* pesan yang akan dibaca. Maka pesan akan melakukan proses Dekripsi.

e) Sistem yang ada di *web server* akan melakukan dekripsi *text* dan *file* dan menghasilkan pesan menjadi *plaintext*.

Berikut ini adalah gambaran alur kerja aplikasi untuk proses penerimaan *email* :



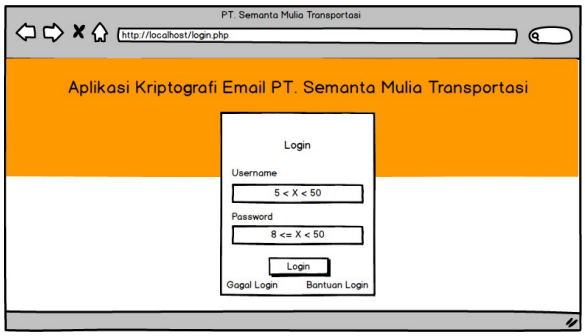
Gambar 2: Alur Proses Penerimaan Email

3.2 Rancangan Layar Program

Rancangan layar merupakan gambaran *prototype program*. Maka dari itu rancangan layar harus sangat mudah dimengerti dan dipahami dalam segi pandang *user* dan penempatan menu-menu aplikasi, dan *user* tidak mengalami kesulitan dan merasa nyaman dalam menjalankan program ini.

a. Rancangan Layar Halaman *Login*

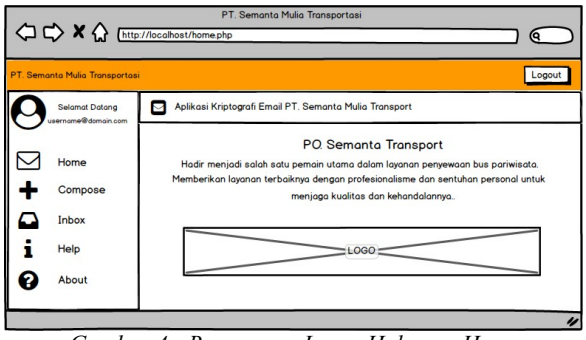
Halaman *Login* adalah halaman dimana *user* melakukan aktifitas memasukan *username* dan *password* yang terdaftar dalam akun *email* gmail / yahoo / outlook.



Gambar 3 : Rancangan Layar Halaman Login

b. Rancangan Layar Halaman *Home*

Halaman *Home* adalah halaman berisikan informasi tentang perusahaan dan logo perusahaan dan menu-menu dari aplikasi ini.



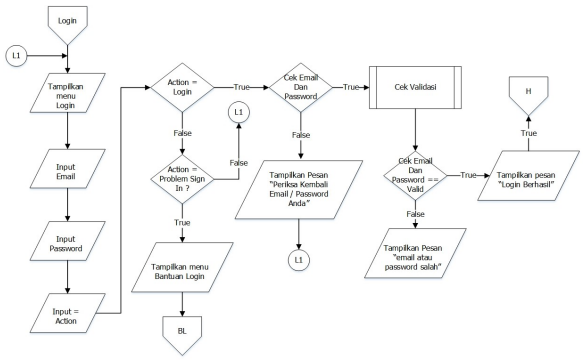
Gambar 4 : Rancangan Layar Halaman Home

3.3 *Flowchart*

Flowchart digunakan untuk menjabarkan cara kerja program untuk memperjelas alur proses, serta algoritma program supaya memudahkan dalam pembuatan dan perancangan program.

a. *Flowchart Login*

Pada *Flowchart form login* user mengisikan *username* dan *password* apabila ingin menggunakan aplikasi

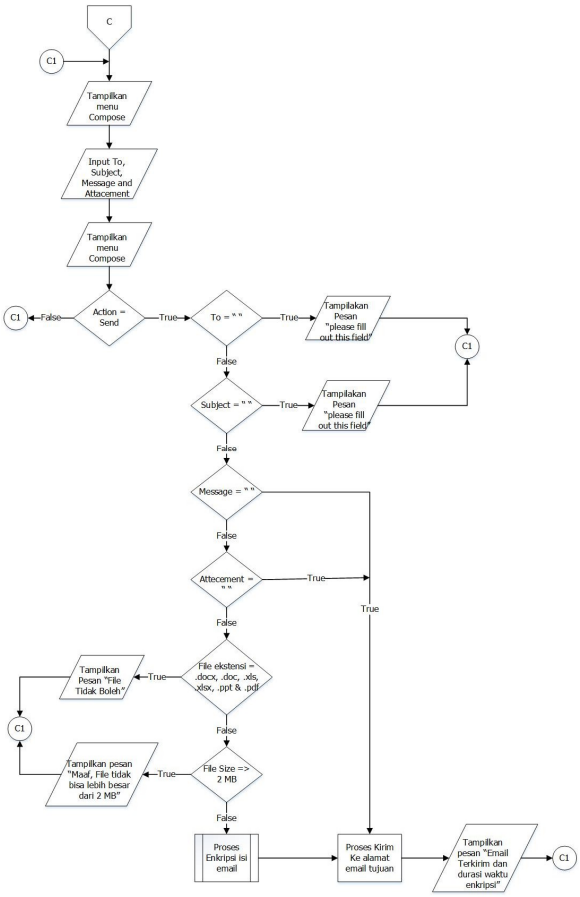


Gambar 5 : Flowchart Form Login

b. *Flowchart Compose*

Pada *flowchart* form ini *user* bisa membuat pesan baru dan mengirimkan kepada penerima. Pengirim meng-*input* alamat *email* penerima, *subject*, isi pesan serta melampirkan *file* jika diperlukan sebelum melakukan pengiriman *email*. Pada proses pengiriman, sistem yang ada diaplikasi akan melakukan proses enkripsi

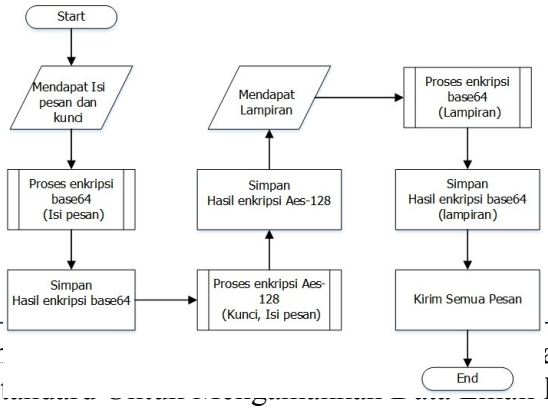
terlebih dahulu yaitu mengunakan metode kriptografi base64 dan *Advanced Encryption Standard*. *Mail server* pengirim akan menyimpan pesan berbentuk *ciphertext* yang telah dikirimkan oleh pengirim.



Gambar 6 : Flowchart Compose

c. *Flowchart* Proses Enkripsi Data *Email*

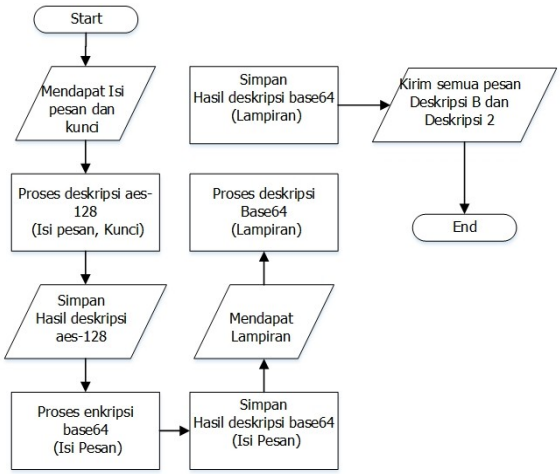
Pada *flowchart form* proses enkripsi data *email*, menjelaskan alur proses enkripsi data *email* yang diawali dengan kriptografi base64 kemudian *Advanced Encryption Standard*. Sedangkan untuk *file attachement* / lampiran dienkripsi dengan metode kriptografi base64. Setelah semua terenkripsi maka *Mail server* pengirim akan menyimpan pesan berbentuk *ciphertext* yang telah dikirimkan oleh pengirim.



Gambar 7 : Flowchart Proses Enkripsi Data Email

d. *Flowchart* Proses Dekripsi Data *Email*

Pada *flowchart form* proses dekripsi data *email*, menjelaskan alur proses dekripsi data *email* yang diawali dengan kriptografi *Advanced Encryption Standard* kemudian base64 lalu. Sedangkan untuk *file attachement* / lampiran didekripsi dengan metode kriptografi base64.



Gambar 8 : Flowchart Proses Dekripsi Data Email

3.4 Algoritma Program

Algoritma digunakan untuk mempermudah dalam pembuatan dan perancangan suatu aplikasi sistem, dimana algoritma ini akan menggambarkancara kerja program. Dibawah ini adalah proses algoritma *form compose*.

```
Tampil Form Compose
Input To, Subject, Message and file Attacement
Input action
    If Action = Send then
      If To = " " then
        Tampilkan "pesan please fill out this field"
    Else if
      If Subject = " " then
        Tampilkan pesan "please fill out this field"
      Else
        Proses Enkripsi isi email
        Proses Kirim ke alamat email tujuan
        Tampilkan pesan "Email Terkirim"
     End If
   End If
  End If
   Kembali ke baris 1
 End If
```

4. HASIL DAN PEMBAHASAN

4.1. Tampilan Layar

Agar aplikasi dapat digunakan dengan mudah, maka tampilan layar yang dibuat haruslah mudah dimengerti oleh pengguna, sehingga pengguna tidak mengalami kesulian dalam menjalankan aplikasi ini.

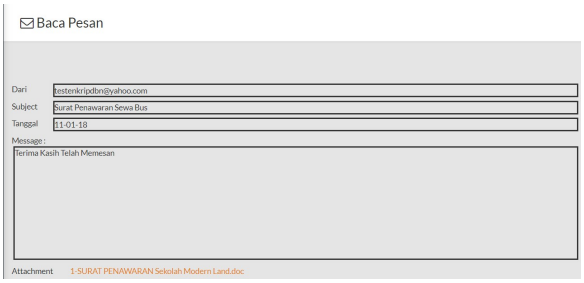
a. Tampilan menu *Login*

Pada saat aplikasi ini dijalankan, *user* harus memasukkan *email* dan *password* yang *valid* dan yang sudah diizinkan kemudian menekan tombol *login*.

Gambar 9 : Tampilan Form Login

b. Tampilan *Inbox* Pesan Menggunakan Aplikasi

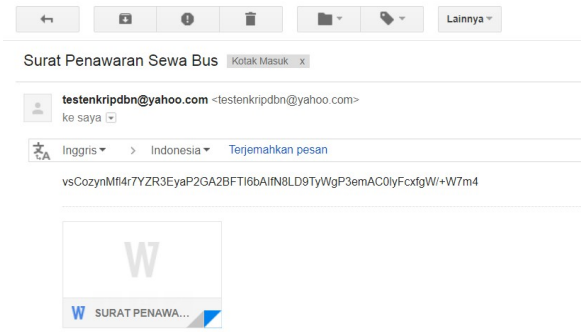
Tampilan *inbox* / baca pesan akan tampil jika *user* sudah *login* aplikasi berhasil. Lalu Pada *form home* pilih menu *inbox,* kemudian pilih pesan yang akan dibaca / dibuka. Setelah itu akan muncul pesan yang sudah dipilih.



Gambar 10 : Tampilan Form Inbox menggunakan aplikasi

c. Tampilan *Inbox* Jika Tidak Menggunakan Aplikasi

Tampilan *inbox* / baca pesan jika tidak menggunakan aplikasi maka hanya isi pesan akan menjadi kata acak / *ciphertext* yang sulit dimengerti dan *file attachement* jika di *download* tidak bisa dibuka atau tidak bisa di mengerti.



Gambar 11 : Tampilan Form Inbox tidak menggunakan aplikasi

4.3. Tabel Pengujian Sistem

Tabel Pengujian Sistem ini bertujuan untuk mengetahui tingkat keberhasilan aplikasi yang telah dibuat. Tabel pengujian sistem pada aplikasi ini akan diuji mengenai waktu yang difokuskan pada proses enkripsi menggunakan kriptografi *base*64 kemudian kriptografi *Advance Encryption Standard*-128, dekripsi dengan kriptografi *Advance Encryption Standard*-128 lalu kriptografi *base*64, dengan menggunakan kunci dari *subject* dan aktivitas lain pada aplikasi. Berikut ini adalah tabel yang memperlihatkan hasil dari pengujian tersebut :

a. Tabel Hasil Pengujian Proses Enkripsi

Berikut ini adalah hasil dari pengujian proses enkripsi data *email* yang ada pada aplikasi ini.

Tabel 1 : Hasil Pengujian Proses Enkripsi

Plain text	Lampiran	Kunci	Ukuran	Waktu	Cipher text
Terima Kasih Telah Memesan	SURAT PENAWARAN Sekolah Modern Land.doc	Surat Penawaran Sewa Bus	304 kb	8.828 detik	vsCozynMfl4r7YZR3EyaP2GA2BFTI6bAIfN8LD9TyWgP3emAC0lyFcxfgW/+W7m4
Invoice Pembayaran	INVOICE PT TAKAGI.pdf	Mohon Segera Dibay	386 kb	11.483 detik	IpDt4MCXCov9hI4QhpjnX/lWI

		arkan. Terima Kasih			VCkapdyY9KiHojHKcYjuHZyBY7ASpSQWC59Hpv7LXVE2Kb08B91YGnfca2G/g==
Perincian Tour Semanta	Cinangnneng SDN Karang Tengah 1.xlsx	Segera di cek kembali	13 kb	0.421 detik	s+1+WmNphroF/8dD0ytsrouGsQadayE7oRJ17s6QYNEkuI8Zlgcj75+y35prTT0o

b. Tabel Hasil Pengujian Proses Dekripsi

Berikut ini adalah hasil dari pengujian proses dekripsi data *email* yang ada pada aplikasi ini

Tabel 2 : Hasil Pengujian Proses Dekripsi

Cipher text	Lampiran	Kunci	Ukuran	Waktu	Plain text
vsCozynMfl4r7YZR3EyaP2GA2BFTI6bAIfN8LD9TyWgP3emAC0lyFcxfgW/+W7m4	1-SURAT PENAWARAN Sekolah Modern Land.doc	Surat Penawaran Sewa Bus	304 kb	16.270 detik	Terima Kasih Telah Memesan
IpDt4MCXCov9hl4QhpjnX/lWIVCkapdyY9KiHojHKcYjuHZyBY7ASpSQWC59Hpv7LXV	2-INVOICE PT TAKAGI.pdf	Mohon Segera Dibayarkan. Terima Kasih	396 kb	18.240 detik	Invoice Pembayaran
E2Kb08B91YGnfca2G/g==					
s+1+WmNphroF/8dD0ytsrouGsQadayE7oRJ17s6QYNEkuI8Zlgcj75+y35prTT0o	Cinangneng SDN Karang Tengah 1.xlsx	Segera di cek kembali	13 kb	6.070 detik	Perincian Tour Semanta

4.3. Analisa Hasil Ujicoba

Analisa program dimaksudkan untuk mengevaluasi hasil dari aplikasi yang telah dibuat. Berdasarkan hasil uji coba diatas, dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi yang dibuat sebagai berikut :

a. Kelebihan Program

1) Program dapat dibuka di browser apapun, sehingga didapatkan tingkat fleksibilitas yang tinggi
2) Tampilan apliasi userfriendly sehingga mudah dipahami.
3) Dapat di buka diberbagai sistem operasi, karena berbasis web.
4) Proses waktu enkripsi dan dekripsi cukup cepat.
5) Pesan tidak dapat dibaca apabila tidak menggunakan aplikasi.
6) Isi pesan akan kembali seperti semula setelah terdekripsi.

b. Kekurangan Program

1) Aplikasi ini hanya dibatasi untuk meng-enkripsi file dengan format doc, docx, ,xls, xlsx dan pdf.
2) Hasil ciphertext isi pesan dan lampiran ukurannya tidak sama.
3) Kecepatan proses enkripsi dan dekripsi tergantung pada ukuran isi pesan dan lampiran. Semakin banyak isi pesan dan semakin besar ukuran lampiran, maka semakin lama proses enkripsi dan dekripsinya.
4) Untuk menjalankan aplikasi membutuhkan koneksi internet yang cepat dan stabil.
5) Jika ada ganggungan saat enkripsi dan dekripsi maka akan terjadi error.
6) Jika mengirim pesan ke Microsoft Outlook maka pesan tidak akan terdekripsi karena

Microsoft mengembangkan proteksi secara otomatis dalam kotak surat. Fitur keamanan premium ini mengaktifkan secara otomatis untuk pelanggan yang memiliki akun email berakhiran @outlook.com, @hotmail.com, @live.com, dan @msn.com dan fitur ini secara default dan tidak dirancang untuk dinonaktifkan.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Melalui proses perancangan, pengerjaan dan serangkaian pengujian, maka dapat di simpulkan beberapa hal dalam aplikasi ini sebagai berikut :

a. Algoritma *Base*64 Algoritma AES dapat diimplementasikan ke dalam bahasa pemrograman PHP untuk melakukan enkripsi dan dekripsi suatu teks dan file.
b. Aplikasi Kriptografi email pada PT. Semanta Mulia Transport tidak memerlukan proses instalasi terlebih dahulu dan dapat dijalankan pada sistem operasi apapun karena berbasis web.
c. Dengan adanya implementasi kriptografi, informasi pesan email yang telah dilakukan proses enkripsi dapat terjaga keamanan dan kerahasiaannya.
d. Informasi pada pesan email dapat di rahasiakan dan di amankan dari penyalahgunaan dan pencurian informasi.

5.2. Saran

Beberapa saran yang dapat di berikan untuk pengembangan lebih lanjut dengan beberapa perkembangan lagi, antara lain :

a. Aplikasi diharapkan dapat ditingkatkan dengan mengkombinasikan beberapa algoritma kriptografi dan kompresi agar dapat memberikan keamanan yang lebih baik dan efisien.
b. Aplikasi diharapkan dapat dikembangkan dengan penambahan fitur-fitur lain di dalamnya.
c. Dapat dikembangkan seperti dapat mengupload file yang lebih banyak dengan ukuran lebih besar tanpa harus memperlambat proses enkripsi dan deskripsi secara signifikan.
d. Lebih banyak lagi menambahkan alamat email seperti AOL, Thunderbird, iPhone, dan melakukan fixed pada Outlook.

DAFTAR PUSTAKA

[1] Niko. 2015. Penjelasan Lengkap Cara Kerja Email Server. Avariable at: http://www.pintarkomputer.com/penjelasan-lengkap-cara-kerja-email-server/?q=/2015/07/penjelasan-lengkap-cara-kerja-email-server.html [Diakses Januari 18, 2018].

[2] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi: teori analisis & implementasi. Edited by F. S. Suyantoro*. Yogyakarta: C.V ANDI OFFSET.

[3] Pabokory, F. N., Astuti, I. F. and Kridalaksana, A. H. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard, Jurnal Informatika Mulawarman, 10(1), pp. 20–31.

[4] Rahardian, A. 2014. Implementasi *Uniform Resource Locator Encryption* Pada *Website* Berbasis Algoritma *Base*64 Studi Kasus Pada Pimpinan Wilayah Aisyiyah Jawa Tengah.

[5] Kromodimoeljo, Sentot. 2009. *Teori & Aplikasi Kriptografi*. Jakarta: SPK IT Consulting.

[6] Primartha, R. 2013. Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma *Advanced Encryption Standard* (AES)*, Journal of Research in Computer Science and Applications*, 2(1), pp. 13–18.