IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128BIT DAN ELGAMAL UNTUK PENGAMANAN E-MAIL PADA BANDARA INTERNASIONAL SULTAN MAHMUD BAHARUDDIN II PALEMBANG

Rizky Tahara Shita[1)], Lauw Li Hin[2)]
[1,2)] Universitas Budi Luhur, Fakultas Teknologi Informasi,
Jl. Ciledug Raya. Petukangan Utara. Jakarta Selatan, Jakarta, 12260
Telp: (021) 5853753, HP: +6285716483190 [1)], +628129743900 [2)]
E-mail: rizky.tahara@gmail.com [1)], lihinwap@gmail.com [2)]

Abstrak

Keamanan dokumen merupakan salah satu hal yang sangat penting dalam pertukaran data dan informasi, khususnya pertukaran data menggunakan media email, karena terdapat banyak ancaman pada saat proses tersebut dilakukan. Keamanan data, khususnya untuk dokumen teks merupakan hal yang sangat penting. Karena teks pesan yang dikirim terkadang adalah pesan yang bersifat rahasia dan pribadi, sehingga kerahasiaan pesan menjadi sangat penting. Keamanan dokumen pada Bandara SMB II sangatlah penting seperti data karyawan dari kantor pusat serta dokumen perusahaan yang tidak boleh diketahui oleh orang luar. Dokumen tersebut merupakan dokumen yang sangat rahasia, jika dokumen penting perusahaan sampai jatuh ke tangan yang tidak bertanggung jawab, maka ada pihak yang akan sangat di rugikan dalam insiden tersebut. Oleh sebab itu, diperlukan tingkat keamanan yang lebih baik dengan dikembangkannya sebuah aplikasi penyandian informasi atau pesan yang akan dikirimkan. Memanfaatkan media email yang ditunjukkan untuk membantu mengatasi masalah keamanan dokumen, agar pihak ketiga tidak dapat mengetahui isi dari informasi atau pesan tersebut. Pemanfaatan algoritma AES 128bit dipadukan dengan algoritma Elgamal untuk menghasilkan sebuah aplikasi penyandian informasi dalam meningkatkan keamanan dokumen.

Kata kunci: *kriptografi, email, aes 128bit, elgamal*

Abstract

Document security is one of the most important things in the exchange of data and information, especially the exchange of data using email media, because there are many threats when the process is done. Data security, especially for text documents is very important. Because the text of messages that are sent is sometimes a private and confidential message, so the confidentiality of messages becomes very important. Document security at SMB II Airport is very important such as employee data from head office as well as company documents that should not be known by outsiders. The document is a very secret document, if the important documents of the company fall into the hands of irresponsible, then there are parties who will be very harmful in the incident. Therefore, a better level of security is required with the development of an encryption application or message to be sent. Utilize the email media shown to help resolve document security issues, so that third parties can not know the contents of the information or messages. Utilization of AES 128bit algorithm combined with Elgamal algorithm to generate an information encoding application in improving document security.

Keywords: *cryptographi, email, aes 128bit, elgamal*

1. PENDAHULUAN

1.1 Latar Belakang

Komunikasi merupakan hal yang penting dalam kehidupan sehari-hari. Komunikasi dapat dilakukan secara langsung maupun tidak langsung. Bentuk komunikasi tidak langsung dapat menggunakan media kertas seperti pengiriman surat-menyurat melalui kantor pos maupun media elektronik seperti email. Namun surat-menyurat melalui kantor pos memerlukan waktu lama untuk lokasi yang jauh, sehingga akan menambah biaya pengiriman. Berbeda dengan email yang hanya membutuhkan koneksi Internet dalam penggunaannya, sehingga tidak membutuhkan waktu lama dalam proses pengiriman yang akan menghemat biaya meskipun lokasi yang dituju sangat berjauhan. Namun email juga rentan terhadap tindakan kejahatan yang membuat email tidak aman untuk berkomunikasi. Email *spoofing*, *sniffing*,

dan *spam* merupakan bentuk kejahatan yang dilakukan pada email. Dari setiap bentuk kejahatan tersebut menimbulkan kerugian tersendiri bagi email, namun bentuk kejahatan sniffing yaitu penyadapan email pada lalu lintas data yang paling banyak mengakibatkan kerugian terbesar dan berbahaya. Hal ini dikarenakan data yang disadap dapat merupakan data-data penting sebuah perusahaan, lembaga atau perorangan. Data-data tersebut bisa dimanfaatkan sendiri oleh penyadap atau diperjual-belikan, sehingga menimbulkan kerugian dari pihak yang di sadap. Keamanan informasi memainkan peran utama dalam aspek transformasi data. Bandara International Sultan Mahmud Badaruddin II Palembang adalah salah satu perusahaan yang dikelola oleh Angkasa Pura II (Persero) yang merupakan salah satu Badan Usaha Milik Negara yang bergerak dalam bidang usaha pelayanan jasa kebandarudaraan dan pelayanan jasa terkait bandar udara di wilayah Indonesia Barat. Keamanan dokumen pada Bandara SMB II sangatlah penting seperti data-data karyawan dari kantor pusat serta dokumen-dokumen perusahaan yang tidak boleh diketahui oleh orang luar. Dokumen tersebut merupakan dokumen yang sangat rahasia, jika dokumen penting perusahaan jatuh ke tangan yang tidak bertanggung jawab, maka ada pihak yang akan sangat dirugikan dalam insiden tersebut. Oleh sebab itu, diperlukan tingkat keamanan yang lebih baik.

1.2 Masalah

Permasalahan yang terjadi selama penelitian:

- Bagaimana melakukan implementasi algoritma AES 128 bit dan Elgamal ke dalam aplikasi pengiriman dokumen menggunakan fitur email?
- Bagaimana cara mengamankan dokumen karyawan dan dokumen penting lainnya yang dikirim melalui email agar terjaga kerahasiaannya?

1.3 Tujuan

Tujuan dari penulisan ini adalah sebagai berikut:

- Mengembangkan suatu aplikasi pengamanan data menggunakan algoritma kriptografi AES 128 bit dan Elgamal untuk mengamankan informasi atau pesan yang sifatnya rahasia.
- Mengamankan file dan pesan yang dikirim atau diterima melalui email agar tidak dapat diketahui oleh orang yang tidak bertanggung jawab melalui email dalam satu aplikasi dengan algoritma AES 128 bit dan Elgamal.
- Menghasilkan aplikasi enkripsi email yang diharapkan mudah dimengerti dan digunakan oleh pengguna.

1.4 Batasan Masalah

Agar penelitian ini tidak keluar dari pembahasan maka diperlukan ruang lingkup masalah, yaitu:

- Algoritma yang digunakan adalah algoritma AES 128 bit dan Elgamal.
- Uji coba file yang digunakan dalam aplikasi ini adalah file dengan ekstensi *.pdf, *.ppt, *.pptx *.xls, *.xlsx, *.doc, *.docx, *.txt.
- Ukuran file maksimal 1 Mb.
- Bahasa Pemrograman yang digunakan yaitu PHP, HTML, JavaScript.

2. LANDASAN TEORI

2.1 Definisi Email

Email (*Electronic Mail*) merupakan salah satu layanan yang tersedia di Internet. Dimana layanan ini digunakan untuk saling korespondensi antar teman, relasi, lembaga dan lain sebagainya. Dengan email; data dikirim secara elektronik, sehingga sampai ditujuan dengan cepat.

Konsep email adalah seperti kita mengirim surat dengan pos biasa, dimana kita mengirimkan ke kantor pos dengan dibubuhi alamat yang dituju. Dari Kantor Pos tersebut akan disampaikan ke Kantor Pos yang terdekat dengan alamat yang dituju dan akhirnya sampai ke alamat tersebut (Gultom,2013).

2.2 Kriptografi

2.2.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, Menurut bahasa tersebut kata kriptografi dibagi menjadi dua, yaitu *kryptos* dan *graphein*. *Kryptos* berarti *secret* (rahasia) dan *graphein* berarti *writing* (tulisan). Menurut teminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari sutau tempat ke tempat yang lain. Dalam perkembangannya, kriptografi digunakan untuk mengidentifkasikan pengiriman pesan dengan tanda tangan digital dan keaslian pesan dengan sidik jari digital (*Fingerprint*) (Purwadi, Jaya, & Calam, 2014).

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Keamanan merupakan bentuk tindakan untuk mempertahankan sesuatu hal dari berbagai macam gangguan dan ancaman (Sianturi, 2013).

Kriptografi selalu terdiri dari dua bagian, yaitu enkripsi dan dekripsi. Enkripsi (*encryption*) merupakan proses yang dilakukan untuk mengubah pesan yang tidak disandikan (*plaintext*) ke dalam bentuk yang tidak dapat dibaca (*ciphertext*). Sedangkan dekripsi (*decryption*) adalah proses kebalikannya. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Suatu sistem yang memiliki algoritma kriptografi, ditambah seluruh kemungkinan *plaintext*, *ciphertext* dan kuncinya disebut dengan kriptosistem (*cryptosystem* atau *cryptographic system*).

2.2.2 Terminologi Kriptografi

Menurut Arjana (2012); terdapat beberapa istilah penting dalam kriptografi, yaitu:

- *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi *ciphertext*.
- Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
- Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

2.2.3 Algoritma Kriptografi

Algoritma kriptografi menurut Purwadi (2014); terdiri dari 3 fungsi dasar, yaitu :

- Enkripsi: merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode yang tidak dimengerti. Enkripsi ini diartikan dengan *cipher* atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata, maka kita akan melihatnya didalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks asli kebentuk teks kode, kita menggunakan algortima yang dapat mengkodekan data yang kita inginkan.
- Deskripsi: merupakan kebalikan dari enkripsi. Pesan yang telah di enkripsi dikembalikan kebentuk asalnya (teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk deskripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
- Kunci: yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*Private Key*) dan kunci umum (*Public Key*).

2.3 AES

Inisiatif *Advanced Encryption Standard* (AES) diumumkan dan pada bulan September 1997 dimana publik diundang untuk mengajukan proposal *block cipher* yang cocok sebagai kandidat untuk AES. Pada tahun 1999 NIST

mengumumkan lima kandidat finalis yaitu MARS, RC6, Rijndael, Serpent, dan Twofish.

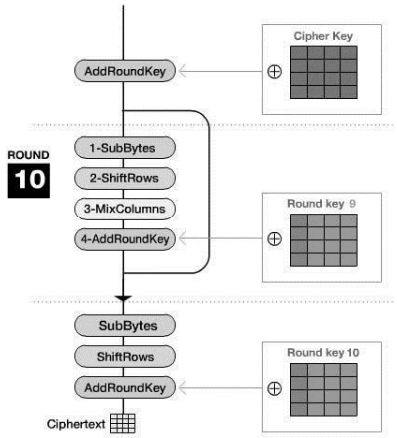
Algoritma AES Rijndael dipilih pada bulan Oktober 2001 dan standarnya diperkenalkan pada bulan November 2002. Algoritma AES ini dipilih sebagai algoritma pengganti DES didasarkan pada tiga kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. Keamanan merupakan faktor utama dalam kriteria ini. Supaya algoritma ini tahan terhadap semua jenis serangan yang telah diketahui maupun belum diketahui. Disamping itu algoritma ini haruslah bebas digunakan tanpa harus membayar royalti. Dalam penerapannya dalam hardware maupun software, algoritma AES harus efisien dan cepat apabila dijalankan dalam berbagai platform 8 bit hingga 64 bit. Algoritma AES dihasilkan dari proses bertahun-tahun yang dipimpin NIST dengan bimbingan dan review dari komunitas internasional pakar kriptografi. Algoritma Rijndael yang dikembangkan oleh Joan Daemen dan Vincent Rijmen dipilih sebagai standar enkripsi.

AES termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu (Sianturi, 2013).

2.3.1 Proses Enkripsi AES 128bit

AES memiliki ukuran blok dan kunci yang tetap sebesar 128, 192, atau 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Blok data masukan dan kunci dioperasikan dalam bentuk array.

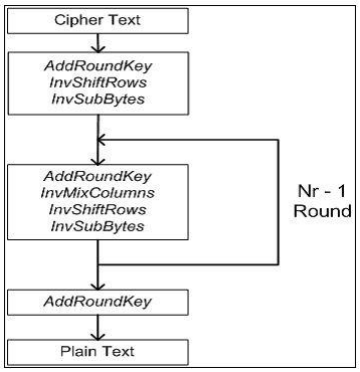
Setiap anggota array sebelum menghasilkan keluaran *ciphertext* dinamakan dengan *state*. Setiap *state* akan mengalami proses yang secara garis besar terdiri dari beberapa tahap yaitu: AddRoundKey ShiftRows, dan MixColumns. Kecuali tahap ketiga tahap lainnya akan diulang pada setiap proses sedangkan tahap MixColumns tidak akan dilakukan pada tahap terakhir. (Sianturi, 2013)



Gambar 1: Algoritma Enkripsi AES (Sianturi, 2013)

2.3.2 Proses Dekripsi AES 128bit

Transformasi dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse dipahami untuk algoritma AES. Transformasi digunakan pada invers cipher pada proses dekripsi AES adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey (Winarno et al., 2012).



Gambar 2: Alogritma Dekripsi AES (Winarno et al., 2012)

2.4 Elgamal

Algoritma ElGamal dibuat oleh Taher ElGamal pada tahun 1984, dan algoritma ini merupakan algoritma yang termasuk dalam kategori algoritma asimetris. Pada awalnya algoritma ini digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi. Algoritma ElGamal mempunyai kunci publik berupa tiga pasang

bilangan dan kunci rahasia berupa dua bilangan. Algoritma ini mempunyai kerugian pada *ciphertext*-nya yang mempunyai panjang dua kali lipat dari *plaintext*-nya. Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. Untuk *plaintext* yang sama, algoritma ini memberikan *ciphertext* yang berbeda pada saat setiap kali *plaintext* tersebut dienkripsi. Hal tersebut dikarenakan adanya pengaruh dari sebuah variabel yang ditentukan secara acak pada saat proses enkripsi dilakukan (Widarma,2016).

Besaran-besaran yang digunakan dalam algoritma kriptografi Elgamal adalah :

- Bilangan prima p bersifat tidak rahasia.
- Bilangan bulat acak g (g < p) bersifat tidak rahasia.
- Bilangan bulat acak x ($1 \leq x \leq p-2$) bersifat rahasia.
- Bilangan y bersifat tidak rahasia.
- m (*Plaintext*) bersifat rahasia merupakan pesan asli yang digunakan sebagai input pada proses enkripsi dan merupakan output dari proses dekripsi.

3. ANALISA MASALAH DAN PERANCANGAN

3.1 Analisa Masalah

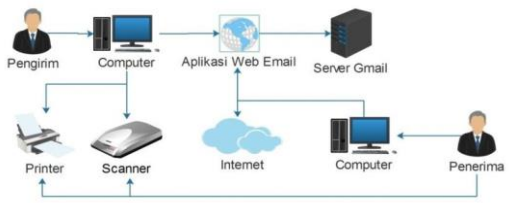
Dalam era modern seperti sekarang, bertukar pesan atau informasi adalah kegiatan yang sudah umum dilakukan setiap hari. Apalagi informasi tersebut dapat dikirimkan melalui media internet seperti Email dan hampir setiap orang mempunyai akun email pribadi, tempat bekerja dan lain sebagainya. Informasi yang dikirimkan tentu merupakan sesuatu yang penting; baik itu informasi umum maupun informasi rahasia, tetapi jika informasi yang dikirimkan tersebut adalah informasi rahasia yang tidak boleh diketahui pihak yang tidak berkepentingan. Tanpa pengamanan yang maksimal informasi atau data tersebut tentu bisa disadap oleh pihak yang tidak bertanggung jawab. Salah satu faktor yang menyebabkan informasi tersebut disadap karena informasi tersebut akan melewati banyak server sebelum sampai tujuan. Hal ini tentu saja menimbulkan masalah baru, terutama masalah pengamanan data bagi suatu instansi yang sebagian besar data atau informasi yang dikirim merupakan rahasia aset instansi.

3.2 Pemecahan Masalah

Dari permasalahan yang diuraikan diatas, dibutuhkan aplikasi email yang dapat menjaga kerahasiaan informasi tersebut dengan menggunakan kriftografi, sehingga membuat penggunanya merasa efisien karena tidak perlu menulis isi pesan, mengenkripsi dan mengirim email dengan aplikasi yang berbeda. Aplikasi ini menggunakan algoritma AES-128 bit dan algoritma Elgamal yang berbasis web. Pesan yang dikirimkan oleh aplikasi ini akan dienkripsi dua kali, pertama menggunakan algoritma AES 128 bit. Hasil enkripsi algoritma AES 128 bit akan dienkripsi lagi menggunakan algoritma Elgamal.

3.3 Analisis Arsitektur Sistem

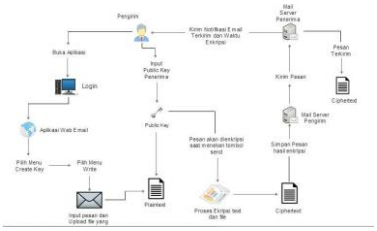
Agar mendapatkan hasil yang berupa aplikasi penyandian informasi, maka dibutuhkan arsitektur sistem dalam memudahkan pada saat pengembangannya. Aplikasi yang dikembangkan adalah berbasis Web, sehingga dibutuhkan Server untuk penempatan aplikasi yang dapat diakses oleh pengirim untuk dapat melakukan penyandian informasi. Dibantu dengan adanya Gmail Server dari Google untuk konektivitas akun, maka penyandian informasi diolah agar memanfaatkan akun Gmail untuk disampaikan kepada penerima. Berikut adalah gambar dari analisa arsitektur sistem tersebut:



Gambar 3: Analisis Arsitektur Sistem

3.3.1 Skema proses pengiriman e-mail

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



Gambar 4: Skema Pengiriman Email

3.3.2 Skema proses penerimaan e-mail

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

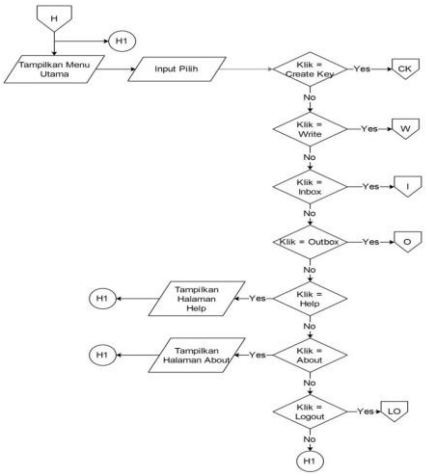
Gambar 5: Skema Penerimaan Email

3.4 Menu Home

Pada halaman utama ini *user* dapat menggunakan aplikasi secara keseluruhan yang terdiri dari satu tombol logout dan enam menu yaitu: menu create key, menu write, menu inbox, menu outbox, menu help dan menu about.

3.4.1 *Flowchart* Menu *Home*

Berikut adalah *flowchart* halaman utama (*home*):



Gambar 6: Flowchart Menu Home

3.4.2 Tampilan Layar Menu *Home*

Tampilan layar menu utama ini merupakan tampilan halaman awal aplikasi setelah melakukan login. Untuk lebih jelasnya berikut adalah gambar tampilan layar menu home:

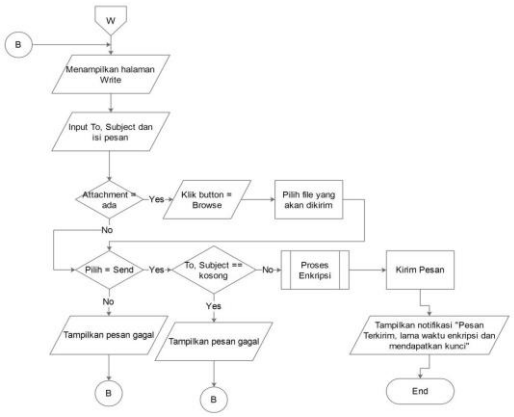
Gambar 7: Tampilan Layar Menu Home

3.5 Menu *Write*

Pada halaman *write*, *user* harus mengisi To, Subject, dan Message. Jika *user* ingin melampirkan file, pilih *browse*. Kemudian isi pesan dan file tersebut akan di enkripsi terlebih dahulu sebelum dikirim ke alamat tujuan.

3.5.1 *Flowchart* Menu *Write*

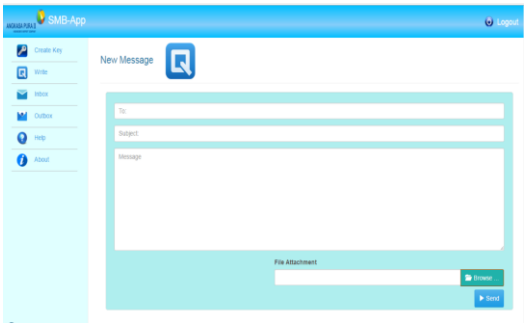
Berikut *flowchart* halaman *write*:



Gambar 8: Flowchart Menu Write

3.5.2 Tampilan Layar Menu *Write*

Fungsi dari menu *write* adalah untuk mengirimkan pesan email ke alamat tujuan. Kemudian pengguna meng-input email tujuan, *subject*, dan *message*. Untuk lebih jelasnya berikut adalah gambar layar menu *write*:



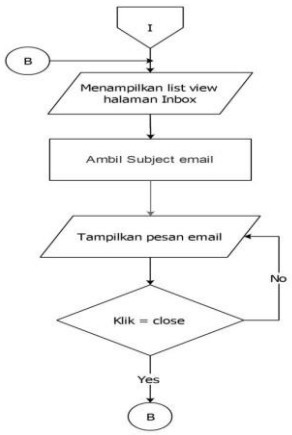
Gambar 9: Tampilan Layar Menu Write

3.6 Menu Inbox

Pada halaman inbox, *user* dapat melihat pesan masuk dari halaman *inbox* dengan memasukkan *private key*. Daftar inbox ini terdiri dari alamat email pengirim, *subject*, waktu pengiriman pesan. Pada halaman *inbox* kita juga dapat men *download* file pada pesan email yang telah diterima.

3.6.1 *Flowchart* Menu *Inbox*

Berikut adalah penjelasan dari *flowchart* halaman *inbox*:



Gambar 10: Flowchart Menu Inbox

3.6.2 Tampilan Layar Menu *Inbox*

Pada tampilan layar ini, pengguna dapat membaca email yang masuk, email akan terbaca dengan cara memilih klik *subject* email. Berikut adalah tampilan layar menu *inbox*:

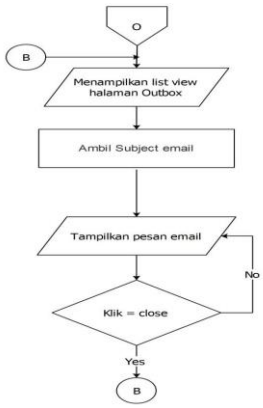
Gambar 11: Tampilan Layar Menu Inbox

3.7 Menu *Outbox*

Pada *flowchart* halaman *outbox*, *user* dapat melihat pesan terkirim dari halaman *outbox*. Daftar *outbox* ini terdiri dari alamat email pengirim, *subject*, waktu pengiriman pesan.

3.7.1 *Flowchart* Menu *Outbox*

Berikut adalah penjelasan dari *flowchart* halaman *outbox*:



Gambar 12: Flowchart Menu Outbox

3.7.2 Tampilan Layar Menu *Outbox*

Pada tampilan layar ini, pengguna dapat membaca email terkirim, email akan terbaca dengan cara memilih klik *subject* email.

Berikut adalah tampilan layar menu *outbox*:

Gambar 13: Tampilan Layar Menu Outbox

3.8 Algoritma AES 128bit

3.8.1 Enkripsi AES 128bit

Pada *flowchart* enkripsi AES 128 adalah mengubah plaintext menjadi *ciphertext*. Langkah awal adalah mengisi plaintext di XOR, setelah di XOR dilakukan proses SubBytes dengan menggunakan tabel s-box; selanjutnya dilakukan proses shiftrows yaitu mengacak dari kanan ke kiri lalu dilakukan proses mixcolumns dengan menggunakan table multiby 2 dan multiby 3, proses diatas dilakukan sebanyak 10 kali, setelah itu dilakukan kembali proses subbytes, shiftrows, lalu antara *state* dengan *roundkey* di XOR barulah mendapatkan hasil *ciphertext*.

1. Start
2. Ciphertext
3. AddRoundKey() = Ciphertext XOR
4. Rounds = 0
5. Rounds = Rounds + 1
6. Proses InvShiftRows ()
7. Proses InvSubBytes ()
8. Proses AddRoundKey() = current state XOR Round Key
9. Proses InvMixColumns ()
10. If Rounds <= 10 Then
11. Kembali ke baris 5
12. Else
13. Proses InvShiftRows ()
14. Proses InvSubBytes ()
15. Proses AddRoundKey() = current state XOR Round Key
16. Output Plaintext
17. End If
18. End

3.8.2 Dekripsi AES 128bit

Dekripsi AES 128 bit adalah mengubah *ciphertext* menjadi *plaintext*. Langkah awal adalah mengisi *ciphertext*, setelah itu InvShiftRows, InvSubBytes, lalu dilakukan AddRoundKey kemudian di XOR, setelah itu di InvMixColumns, InvShiftRows, InvSubBytes dan AddRoundKey kembali, barulah mendapat *plaintext*.

1. Start
2. Plaintext
3. AddRoundKey() = Plaintext XOR
4. Rounds = 0
5. Rounds = Rounds + 1
6. Proses SubBytes()
7. Proses ShiftRows()
8. Proses MixColumns()
9. Proses AddRoundKey() = current state XOR Round Key
10. If Rounds <= 10 Then
11. Kembali ke baris 5
12. Else
13. Proses SubBytes()
14. Proses ShiftRows()
15. Proses AddRoundKey() = current state XOR Round Key
16. Output Ciphertext
17. End If
18. End

3.9 Algoritma Elgamal

3.9.1 Enkripsi Elgamal

Algoritma ini menjelaskan alur jalannya proses algoritma elgamal melakukan enkripsi data

sehingga menjadi *ciphertext*. Untuk lebih jelasnya berikut proses dari algoritma proses enkripsi elgamal:

1. Start
2. Proses enkripsi elgamal
3. Menggunakan kunci publik (p, g, y) , private (p,x) dan (k)
4. Input file
5. Ubah nilai blok file kedalam nilai ASCII
6. Hitung a = g ^ k mod p
7. Hitung b = y ^ k * m mod p
8. Mendapatkan hasil file enkripsi
9. End

3.9.2 Dekripsi Elgamal

Algoritma ini menjelaskan alur jalannya proses algoritma Elgamal melakukan proses dekripsi untuk mengembalikan file yang berupa *ciphertext* menjadi file *plaintext*. Untuk lebih jelasnya berikut algoritma proses dekripsi Elgamal :

1. Start
2. Proses dekripsi elgamal
3. Menggunakan kunci publik (p, g, y) , private (p,x) dan (k)
4. Input file
5. Hitung mi = bi.ai ^ p-1-xmod p
6. Ubah niali blok file kedalam nilai ASCII
7. Mendapatkan hasil file dekripsi
8. End

4. HASIL IMPLEMENTASI DAN ANALISA PROGRAM

4.1 Implementasi

Agar aplikasi pengamanan email berbasis web berjalan dengan baik, spesifikasi perangkat yang digunakan untuk implementasi aplikasi ini juga harus mendukung. Spesifikasi *hardware* yang digunakan pada saat pembuatan aplikasi ini, diantaranya adalah:

- Processor: Intel® Core™ i3
- Memory: 2 GB
- Harddisk: 500 GB

Software yang digunakan dalam uji coba pada hardware di atas memiliki spesifikasi, yaitu:

- Operating System: Microsoft Windows 7 Ultimate 32-bit
- WEB Server : Apache
- Pemrograman: PHP
- Database: MySQL

4.2 Hasil Pengujian

Pengujian program dilakukan setelah kebutuhan terpenuhi baik *hardware* maupun *software*. Pada bagian ini dapat diuraikan mengenai pengujian enkripsi dan dekripsi. Dilakukannya pengujian program adalah untuk mendapatkan hasil perbandingan dari file asli dan file hasil kriptografi.

4.2.1 Proses Enkripsi

Pengujian proses enkripsi merupakan teks yang akan dienkripsi dari *plainteks* menjadi *chiperteks*.

Nama File	**Ukuran Asli (KB)**	**Ukuran Hasil Enkripsi (KB)**	**Waktu Proses (detik)**
Lamaran Kerja.docx	19	27	2.002
Etika Menggunakan Facebook.pdf	120	160	4.147
Presentation Bahasa Inggris.pptx	1.002	1.336	12.870
Rika Anggraini.xlsx	10	14	5.431
Universitas Budi Luhur.doc	131	175	25.793
Gaji pokok.xls	25	33	6.621
Tranp_ai_bab3.ppt	757	1.010	88.361

Tutorial.txt	4	5	4.314

Pada tabel tersebut dapat dilihat kecepatan dari proses enkrip untuk beberapa jenis file yang mana semakin besar file yang dilakukan untuk diproses, maka waktu untuk memprosesnya juga semakin lama. Hal ini juga dipengaruhi oleh jenis file yang diproses dan *hardware* yang digunakan dalam melakukan pengujian; dimana semakin besar kapasitas RAM dan semakin cepat *processor* nya, semakin singkat waktu yang dibutuhkan dalam melakukan proses enkripsi.

4.2.2 Proses Dekripsi

Pengujian proses dekripsi merupakan teks yang akan didekripsi dari *chipertext* menjadi *plainteks*.

Nama File	**Ukuran Asli (KB)**	**Ukuran Hasil Enkripsi (KB)**	**Waktu Proses (detik)**
Lamaran Kerja.docx	27	19	0.004
Etika Menggunakan Facebook.pdf	160	120	0.017
Presentation Bahasa Inggris.pptx	1.336	1.002	0.039
Rika Anggraini.xlsx	14	10	0.009
Universitas Budi Luhur.doc	175	131	0.028
Gaji pokok.xls	33	25	0.005
Tranp_ai_bab3.ppt	1010	757	0.007
Tutorial.txt	5	4	0.012

Proses dekripsi memiliki waktu proses yang lebih cepat dibandingkan proses enkripsi, hal ini dikarenakan dari algoritma dekripsi itu sendiri yang memiliki proses lebih singkat dibandingkan dengan pada saat melakukan enkripsi. Jenis file dan *hardware* juga faktor yang mempengaruhi kecepatan dalam proses dekripsi ini.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisa yang telah dilakukan terhadap permasalahan dan program yang dikembangkan, maka dapat ditarik kesimpulan:

- Dengan adanya aplikasi kriptografi, proses penyimpanan dan pertukaran informasi menjadi lebih aman.
- Waktu yang diperoleh untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang diproses (semakin kecil ukuran file yang diproses, semakin cepat proses enkripsi dan dekripsinya; semakin besar ukuran file, semakin lama proses enkripsi dan dekripsinya). Faktor *hardware* juga menjadi penentu dalam kecepatan proses kriptografi ini.
- Meminimalisir kemungkinan pencurian data oleh pihak yang tidak bertanggung jawab.

5.2 Saran

Selain menarik beberapa kesimpulan, dapat pula diajukan saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan sistem, antara lain:

- Menambahkan fitur lain sesuai dengan kebutuhan.
- Dibutuhkan perawatan dan pengawasan serta pemeliharaan sistem yang telah dibangun agar sistem berjalan dengan baik dan lancar.

6. DAFTAR PUSTAKA

[1] Arjana, P.H. & Rahayu, T.P., 2012. *Implementasi Enkripsi Data dengan Algoritma Vigenere Chiper*. Sentika , pp.164–169 ; ISSN : 2089–9815.

[2] Busran & Mandarani, P., 2012. *Analisis Komputasi Enkripsi dan Dekripsi Data Gambar, Teks dan Audio Dengan Menggunakan Algoritma Rc4 berbasis*

Visual Basic 6.0. , 5, pp.32–45 ; ISSN : 2086–4981.

[3] Gultom, H., 2013. *Penyandian Email Menggunakan Algoritma Kriptografi Wake (Word Auto Key Encryption)*. , IV, pp.107–111 ; ISSN : 2301–9425.

[4] Mahmuzallani, 2016. *Implementasi Kriptografi pada Aplikasi Email Menggunakan Algoritma Elgamal berbasis Android*. , 1, pp.22–26 ; ISSN : 2527–9858.

[5] Purwadi, Jaya, H. & Calam, A., 2014. *Aplikasi Kriptografi Asimetris dengan Metode Diffie-Hellman dan Algoritma Elgamal Untuk Keamanan Teks.* , 13, pp.183–196 ; ISSN : 1978–6603.

[6] Sianturi, F.A., 2013. *Perancangan Aplikasi Pengamanan Data dengan Kriptografi Advanced Encryption Standard (Aes)*. , IV, pp.42–46 ; ISSN : 2301–9425.

[7] Widarma, A., 2016. *Dalam Skema Hybrid untuk Keamanan Data* Adi Widarma. , 1, pp.1–8 ; ISSN : 2502–7131.

[8] Winarno, Puspita Sari S., 2012. *Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard*. , IV, pp.24–32 ; ISSN : 2085–4552.