APLIKASI EMAIL (*Electronic Mail*) MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-128) DAN ALGORITMA *RIVEST CIPHER 4* (RC4) BERBASIS WEB

Ryfan Aditya Indra[1)], **Wahyu Pramusinto, M.Kom**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : ryfandotnet@gmail.com[1)], wahyu.pramusinto@budiluhur.ac.id[2)]

Abstrak

Era teknologi informasi dari masa ke masa mengalami perkembangan yang sangat pesat, diantaranya kemampuan komputer mengalami perkembangan yang signifikan. Teknologi komputer inilah yang sangat dibutuhkan oleh manusia, baik itu untuk individu maupun kelompok. Namun, dalam semua hal aktivitas yang akan dikomputerisasikan diperlukan keamanan data demi menjaga data khususnya data penting untuk kerahasiaan informasi dari isi data tersebut. Ketersediaan keamanan data dapat memicul hal-hal yang lebih baik. Keamanan data dapat dilakukan dengan cara teknik penyamaran atau penyandian data yang saat ini disebut dengan kriptografi. Kriptografi merupakan ilmu dan seni teknik penyamaran atau penyandian pesan untuk melindungi data dengan mengubah kode tertentu dan hanya orang tertentu (encryptor) mempunyai kunci yang dapat menjamin kerahasiaan data. Seperti pada Laboratorium ICT Terpadu Univeristas Budi Luhur yang mengirimkan informasi melalui email dengan utuh tanpa adanya pengamanan lebih. Untuk melakukan keamanan data ataupun informasi maka digunakanlah metode kriptografi. Kriptografi ini akan digunakan sebagai pengamanan lebih dalam pengiriman informasi melalui email. Konsep kriptografi sendiri memiliki empat komponen diantaranya plaintext, ciphertext, key digunakan untuk penyandian dan algoritma sebagai metode enkripsi dan dekripsi. Pada metode kriptografi yang digunakan yakni Algoritma Advanced Encryption Standard dengan jumlah bit 128 (AES-128) dan Algoritma Rivest Cipher 4 (RC4). Dengan menerapkan algoritma tersebut suatu informasi akan diubah isinya menjadi suatu informasi yang tidak dapat dimengerti oleh siapapun dan diharapkan keamanan dalam pengiriman informasi melalui email dapat terjamin kerahasiaan dari sebuah informasi tersebut.

Kata kunci: Algoritma *Advanced Encryption Standard* (AES-128), Algoritma *Rivest Cipher 4* (RC4), *Email*

1. PENDAHULUAN

1.1. Latar Belakang

Era teknologi informasi dari masa ke masa mengalami perkembangan yang sangat pesat, diantaranya kemampuan komputer mengalami perkembangan yang signifikan. Teknologi komputer inilah yang sangat dibutuhkan oleh manusia, baik itu untuk individu maupun kelompok. Dahulu, untuk berkomunikasi sangatlah sulit, namun dengan seiringnya waktu berjalan munculah era teknologi informasi yang dapat mempermudah berkomunikasi. Namun, dalam semua hal aktivitas yang akan dikomputerisasikan diperlukan keamanan data demi menjaga data khususnya data penting untuk kerahasiaan informasi dari isi data tersebut.

Laboratorium ICT Terpadu merupakan sebuah tempat laboratorium komputer yang digunakan untuk menunjang matakuliah praktikum Universitas Budi Luhur. Proses kegiatan belajar-mengajar dan ujian akhir semester matakuliah praktikum tetap dilakukan di Laboratorium ICT Terpadu. Dalam hal ini proses pengiriman jawaban ujian hanya menggunakan aplikasi email dari *Google* yakni *Google Mail* atau yang biasa disebut dengan *Gmail*. Dalam hal ini, Jika seseorang mengetahui *user email* dan *password* dari *email* yang digunakan Laboratorium ICT Terpadu maka sang pelaku langsung mendapatkan informasi dari isi email tersebut tanpa adanya enkripsi data atau pesan *email*. Sehingga diperlukannya keamanan data atau informasi untuk mengamankan informasi pesan atau data dari pihak yang tidak berwenang. Berdasarkan latar belakang tersebut adalah untuk membuat suatu program aplikasi kriptografi dengan algoritma *Advanced Encryption Standard* (AES-128 bit) dan algoritma *Rivest Cipher 4* (RC4) untuk menjaga kerahasiaan data atau pesan *email* agar tidak dapat diketahui isi dari data atau pesan tersebut oleh pihak yang tidak mempunyai wewenang.

2. LANDASAN TEORI

2.1. Definisi Kriptografi

Kriptografi berasal dari dua kata Bahasa Yunani, yakni *Crypto* yang berarti rahasia (*secret*) dan *Grapho* yang berarti menulis (*writing*). Secara umumnya kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Kriptografi mendukung kebutuhan dari dua buah aspek keamanan informasi, yakni *secrecy* yang berarti perlindungan terhadap kerahasiaan pesan/data informasi dan *authenticity* yang berarti perlindungan terhadap pengubahan & pemalsuan informasi yang tidak diinginkan. Kriptografi juga tidak berarti hanya

memberikan keamanan informasi saja, namun kriptografi lebih ke arah teknik-tekniknya. [1]

Konsep kriptografi yang bertujuan untuk menjaga kerahasiaan pesan/data adalah dengan cara menyamarkan pesan/data menjadi bentuk tersandi yang tidak dapat dibaca oleh siapapun. Pesan/data yang akan disandikan disebut *plaintext*, sedangkan yang telah disamarkan (telah disandikan) disebut *ciphertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut dengan enkripsi, sedangkan proses pengembalian dari *ciphertext* menjadi *plaintext* disebut dengan dekripsi. [5]

Kriptografi memiiki 4 komponen utama yaitu:

1) *Plaintext*, yaitu pesan/data yang dapat dibaca.
2) *Ciphertext*, yaitu pesan/data sandi acak yang tidak bisa dibaca oleh siapapun.
3) *Key*, yaitu metode untuk melakukan teknik kriptografi sebagai kunci.
4) Algoritma, yaitu metode untuk melakukan proses enkripsi dan proses dekripsi.

Adapun contoh Teknik Kriptografi Klasik yang dibagi menjadi dua yakni:

1) Kriptografi Subtitusi merupakan teknik mengganti satu atau sekumpulan bit pada blok *plaintext* tanpa mengubah urutannya.
2) Kriptografi Transposisi merupakan teknik memindahkan posisi bit pada blok *plaintext* berdasarkan aturan-aturan tertentu.

Sedangkan contoh dari Teknik Kriptografi Modern sendiri dibagi menjadi 3 yakni:

1) Kriptografi Simetris, yakni teknik enkripsi dan dekripsi dengan metode atau teknik atau kunci yang sama.
2) Kriptografi Asimetris, yakni teknik enkripsi dan dekripsi dengan dua buah kunci yakni kunci publik (*Public key*) dan kunci rahasia (*Private key*).
3) Kriptografi *Hybrid*, yaitu teknik enkripsi dan dekripsi dua lapis, maksud dari dua lapis yaitu setelah *file* di enkripsi kemudian dilakukan enkripsi sekali lagi begitu sebaliknya untuk dekripsinya. [2]

2.2. E-MAIL (Electronic Mail)

Electronic mail (*E-mail*) atau surat elektronik ini merupakan sebuah metode mengubah, menyimpan, mengirim, dan menerima pesan melalui sistem komunikasi elektronik. Istilah *e-mail* (*Electronic Mail*) ini meliputi sistem yang berdasar pada SMTP *(Simple Mail Transfer Protocol*) dan sistem intranet yang memungkinkan untuk pengguna dalam satu organisasi mengirimkan pesan kepada satu sama lainnya. Seringkali pada kelompok organisasi tersebut menggunakan IP (*internet protocol*) sebagai layanan *e-mail* (*Electronic Mail*) internal. Format dari sebuah pesan *e-mail* (*Electronic Mail*) dari internet didefinisikan di RFC 2822 (*Internet Standard*) dan seri dari RFC yang secara keseluruhan disebut sebagai MIME (*Multipurpose Internet MailExtensions)*. Sebuah pesan *e-mail* (*Electronic Mail*) terdiri dari dua bagian besar antara lain:

a. *Header* (Kepala *Email*)

Disusun menjadi beberapa bagian (*field*), umumnya nama *field* ini dimulai dari karakter pertama pada suatu baris, kemudian diikuti oleh tanda ‘:’ (titik dua), lalu diikuti oleh nilai *non-null* (tidak boleh kosong), bukan spasi atau bukan tab pada karakter pertamanya. Nama *field* dan nilainya masuk dalam karakter ASCII (*American Standard Code for Information Interchange*) sebesar 7 bit. Bagian *header* (kepala *email*) dan *body* (badan *email*) dipisahkan oleh satu baris kosong. Pesan pada umumnya paling sedikit memiliki 4 *field* berikut :

1) *From* (Dari): Alamat pengirim *e-mail* dan terkadang diikuti nama pengirim pesan.
2) *To* (Kepada): Tujuan alamat *e-mail* yang akan dikirim dan terkadang diikuti nama penerima pesan.
3) *Subject* (Judul Pesan): Rangkuman isi pesan.
4) *Date* (Tanggal): Waktu dan tanggal setempat saat pesan dikirim.

b. *Body* (Badan *Email*)

Pesan yang diterima berupa teks/gambar tanpa struktur, terkadang mengandung tanda pengenal di bagian akhir. Pada awalnya didesain menggunakan 7 bit ASCII (*American Standard Code for Information Interchange*), tetapi sekarang sebagian besar menggunakan 8 bit, namun belum bersifat umum (*universal)*. [4]

2.3. Algoritma AES (Advanced Encryption Standard)

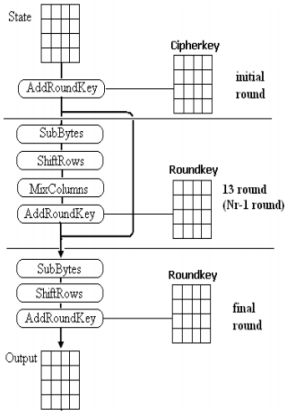
Algoritma AES (*Advanced Encryption Standard*) merupakan algoritma blok *cipher* yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES (*Advanced Encryption Standard*) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES (*Data Encryption Standard*) yang sudah dianggap kuno dan mudah dibobol.

Masukan (*Input)* dan keluaran (*output)* dari algoritma AES (*Advanced Encryption Standard*) terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. Panjang kunci dari AES (*Advanced Encryption Standard*) terdiri dari panjang kunci 128 bit (16 karakter), 192 bit (24 karakter), dan 256 bit (32 karakter). Perbedaan panjang kunci ini yang nantinya mempengaruhi

jumlah putaran pada algoritma *Advanced Encryption Standard* (AES) ini. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada tabel di bawah. [1]

Tabel 1: Jumlah Putaran pada Algoritma Advanced Encryption Standard (AES)[1]

Tipe	Panjang Kunci	Panjang Blok Input	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14



Gambar 1. Proses Enkripsi Pada AES [3]

Garis besar algoritma *Advanced Encryption Standard* (AES) yang beroprasi pada blok 128-bit dengan kunci 128-bit (diluar proses pembangkitan *roundkey*) adalah sebagai berikut :

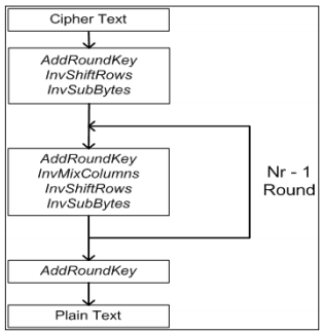
1) *AddRoundKey* yakni melakukan XOR antara awal (*plaintext*) dengan *cipher key*.
2) Putaran sebanyak Nr-1 kali.

Proses yang dilakukan pada setiap putaran adalah :

a. *SubBytes*, yakni subsitusi *byte* menggunakan *table* subsitusi (S-Box).
b. *ShiftRows*, yakni pergeseran baris-baris *array state* secara *wrapping*.
c. *MixColumns*, yakni mengacak data di masing-masing kolom *array state*.
d. *AddRoundKey*, yakni melakukan XOR antara *state* saat *round key*.

3) *Final round*, proses untuk putaran terakhir meliputi:
a. *SubBytes*
b. *ShiftRows*
c. *AddRoundKey* [3]

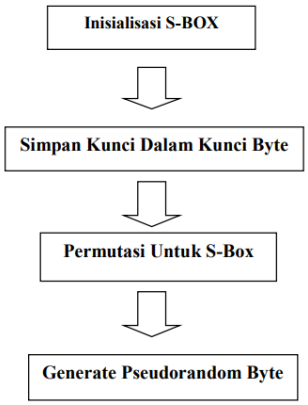
Transformasi pada *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES (*Advanced Encryption Standard*). Transformasi *byte* yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey*. Proses algoritma dekripsi pada AES (*Advanced Encryption Standard*) dapat dilihat pada gambar 2 [3]



Gambar 2. Proses Dekripsi Pada AES [3]

2.4. Algoritma RC4 (Rivest Cipher 4)

RC4 (*Rivest Cipher 4*) merupakan algoritma kriptogrtafi *cipher stream* aliran yang digunakan secara luas pada sistem keamanan seperti protocol SSL (*Secure Socket Layer)*. Algoritma RC4 (*Rivest Cipher 4*) kriptografi ini sederhana dan mudah diimplementasikan. RC4 (*Rivest Cipher 4*) dibuat oleh Ron Rivest dari laboratorium RSA (RC adalah singkatan dari Ron's Code). RC4 (*Rivest Cipher 4*) membangkitkan *keystream* yang kemudian di-XOR-kan dengan *plaintext* pada waktu enkripsi (atau di-XOR-kan dengan bit-bit *ciphertext* pada waktu dekripsi). RC4 (*Rivest Cipher 4*) tidak seperti *cipher stream* aliran yang memproses data dalam bit. RC4 memproses data dalam ukuran byte (1 byte = 8 *bit*). RC4 (*Rivest Cipher 4*) menggunakan dua buah kotak substitusi (S-box) *array* 256 *byte*. [6] Gambar 3 memperlihatkan rangkaian proses yang dijalankan untuk mengenkripsi data.



Gambar 3. Rangkaian Proses Pada RC4 [6]

a. Proses Enkripsi & Dekripsi RC4
1) Inisialisasi terhadap *array* S-box pertama, S[0], S[1], S[2], …., S[255], diisi dengan bilangan 0 sampai 225 sehingga array S-box *array* S berbentuk S[0] = 0, S[1] = 1, …, S[255] = 255.Proses inisialisasi Sbox (*array* S): For r = 0 to 255, S[r] = r
2) Inisialisasi terhadap *array* kunci (S-box lain), misalnya pada *array* kunci K dengan panjang 256. Jika panjang kunci kurang dari 256, dilakukan padding, yaitu penambahan *byte* sehingga panjang kunci

menjadi 256 *byte*. Misalnya, K = abc (hanya 3 *byte* atau huruf), lakukan padding dengan penambahan *byte* (huruf) semu, contohnya K = abcabcabc…. sampai panjang K mencapai 256 byte sehingga S-box array kunci K berbentuk K[0], K[1], K[2], …., K[255]. Proses inisialisasi S-box (*array* K): Array kunci // panjang kunci "*length*".
For i = 0 to 255,
K[i] = Kunci [i mod length].

3) Melakukan permutasi terhadap nilai-nilai di dalam array S dengan cara menukarkan isi array S[i] dengan S[i]. Prosesnya adalah sebagai berikut :
j = 0, for i = 0 to 255,
j = (j + S[i] mod 256,
isi S[i] dan isi S[j] ditukar.
4) Membangkitkan *keystream* dan melakukan enkripsi. Proses untuk membangkitkan kunci enkripsi adalah sebagai berikut :
i = j = 0, i = (i + 1) mod 256,
j = (j + S[i]) mod 256,
isi S[i] dan S[j] ditukar,
t = S[t].
5) *Keystream* K kemudian digunakan untuk mengenkripsikan *plaintext* ke-idx sehingga didapatkan *ciphertext*, sedangkan untuk mendapatkan *plaintext*, XOR-kan *ciphertext* dengan kunci yang sama dengan proses enkripsi. [6]

3. RANCANGAN SISTEM DAN APLIKASI

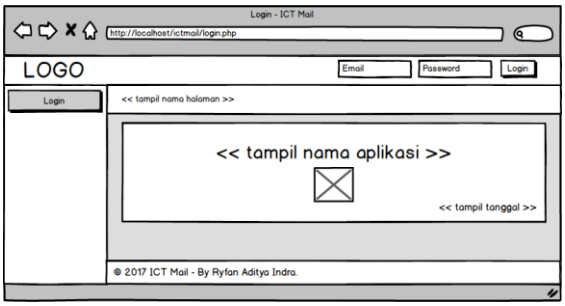
3.1. Rancangan Layar

Program yang akan dibuat terdiri dari 7 halaman yakni Halaman *Index* atau *Login*, Halaman *Home* atau *Dashboard*, Halaman Kirim *Email* atau *Compose*, Halaman Pesan Masuk atau *Inbox*, Halaman Lihat Pesan atau *View Mail*, Halaman Bantuan Penggunaan atau *Help*, Halaman Tentang Aplikasi atau *About*.

Dalam penggunaan aplikasi enkripsi dan dekripsi *email*, pengguna (*user*) wajib melalukan *login* dengan *email Google* (*Gmail*), pengguna sebelumnya mewajibkan *Allow less secure apps* aktif atau ON sebagai perizinan menggunakan aplikasi dengan *user email* yang digunakan. Setelah itu *user* diarahkan ke halaman beranda (*dashboard*) sebagai tanda bahwa *user* telah melakukan autentikasi *user email*. Untuk menggunakan aplikasi pengiriman *email* yang terenkripsi, pengguna dapat memilih menu Kirim *Email* dibagian *sidebar* halaman tepat dibawah menu beranda (*dashboard*). Pengguna (*user*) mengisikan *form* kirim *email* dengan *input*an tujuan *email*, judul pesan, isi pesan, lampiran dan memberikan *password* pesan sebagai kunci dalam mengenkripsi dan memproses serta mengirim *email* menggunakan *SMTP* (*Simple Mail Transfer Protocol*) *Gmail* yang dipadu dengan Algoritma *Advanced Encryption Standard* (AES-128) dan *Rivest Cipher 4* (RC4).

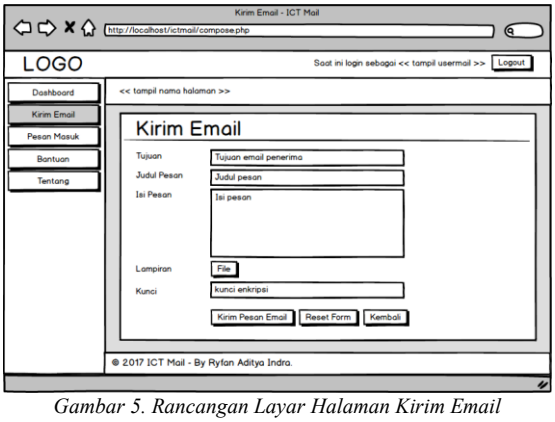
Untuk membaca *email* yang telah dienkripsi menggunakan Algoritma *Advanced Encryption Standard* (AES-128) dan *Rivest Cipher 4* (RC4), pengguna memilih *email* di menu Pesan Masuk atau *Inbox* kemudian akan diarahkan ke halaman Lihat Pesan atau *View Mail*, sebelum membuka isi *email*, pengguna dimintai kunci pertama kali dibuat untuk mendekripsi pesan dan lampiran.

Gambar 4 berikut ini adalah rancangan layar halaman *Login* yakni dimana *user* harus melakukan penginputan *usermail* dan *password*.



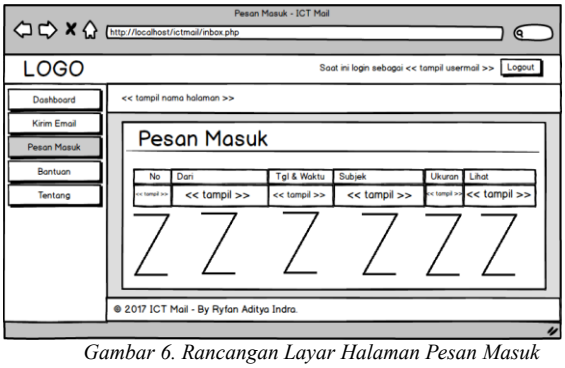
Gambar 4. Rancangan Layar Halaman Login

Kemudian Gambar 5 merupakan rancangan layar halaman Kirim *Email*, dimana *user* harus menginputkan alamat tujuan, subjek pesan, isi pesan, lampiran dan kunci enkripsi.



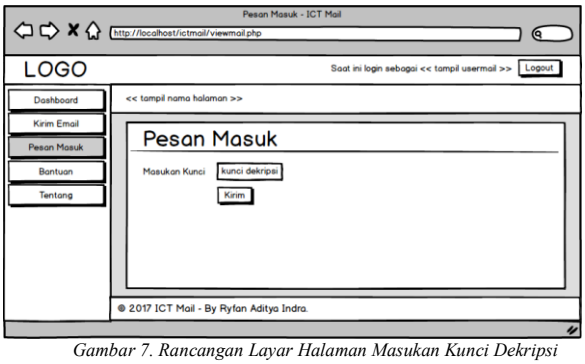
Gambar 5. Rancangan Layar Halaman Kirim Email

Gambar 6 merupakan rancangan layar halaman Pesan Masuk, yakni *user* dapat melihat isi pesan masuk yang ada.

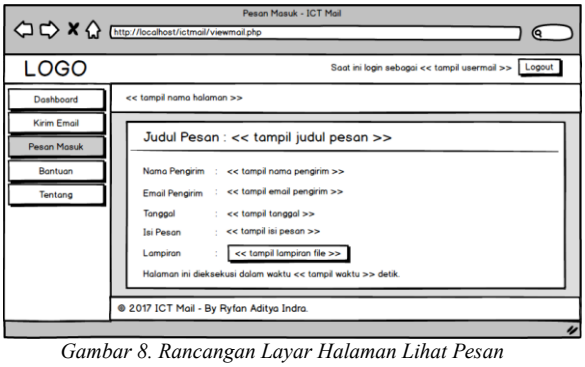


Gambar 6. Rancangan Layar Halaman Pesan Masuk

Gambar 7 dan Gambar 8 merupakan halaman untuk membaca pesan, dimana untuk gambar 7 merupakan halaman untuk penginputan kunci dekripsi dan gambar 8 merupakan halaman menampilkan isi pesan.



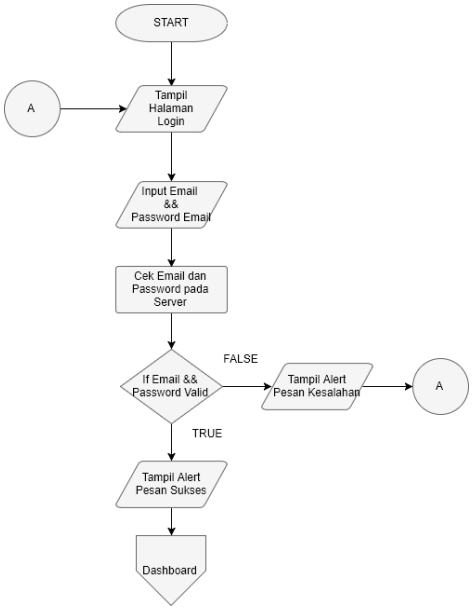
Gambar 7. Rancangan Layar Halaman Masukan Kunci Dekripsi



Gambar 8. Rancangan Layar Halaman Lihat Pesan

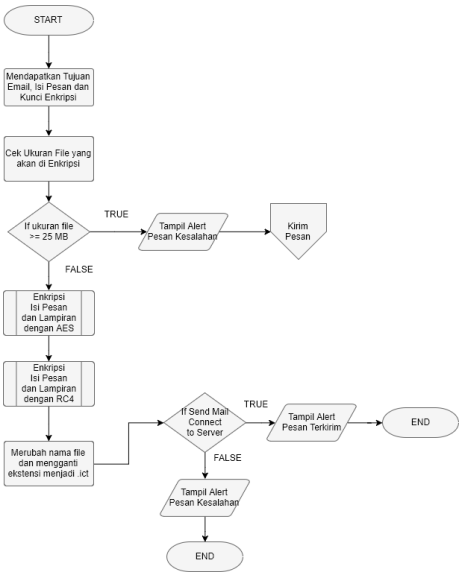
3.2. Flowchart Program

Pada gambar 9 menggambarkan proses yang terjadi pada halaman *login*. Jika benar memasukan *usermail* dan *password* maka akan diarahkan ke menu *dashboard*. Jika tidak akan tampil pesan *error*.



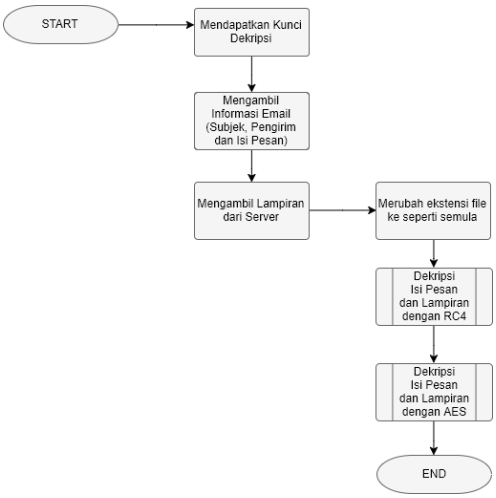
Gambar 9. Flowchart Proses Login

Gambar 10 merupakan alur proses dalam mengirim *email* terenkripsi.



Gambar 10. Flowchart Proses Kirim Email

Kemudian untuk gambar 11 merupakan alur proses dalam mendekripsi pesan untuk melihat pesan yang terenkripsi.

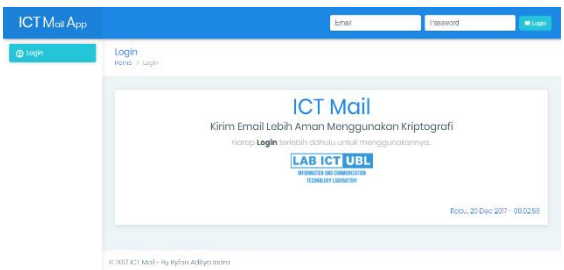


Gambar 11. Flowchart Proses Dekripsi Pesan

4. HASIL DAN PEMBAHASAN

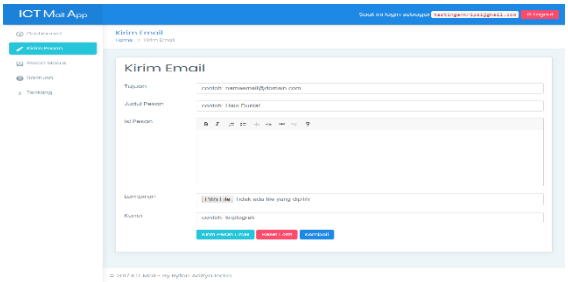
4.1. Tampilan Layar

Gambar 12 adalah tampilan layar utama, user wajib melakukan *login* untuk menggunakan aplikasi.



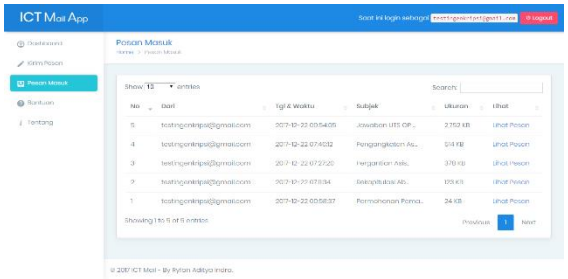
Gambar 12. Tampilan Layar Halaman Login

Gambar 13 merupakan tampilan layar halaman Kirim *Email*, *user* wajib memasukan alamat *email* yang dituju, subjek pesan, isi pesan, lampiran dan kunci enkripsi.



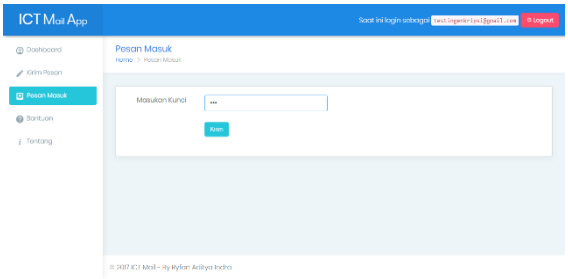
Gambar 13. Tampilan Layar Halaman Kirim Email

Gambar 14 adalah tampilan layar halaman Pesan Masuk dimana *user* dapat melihat pesan-pesan yang masuk yang bertujuan ke email *user*.

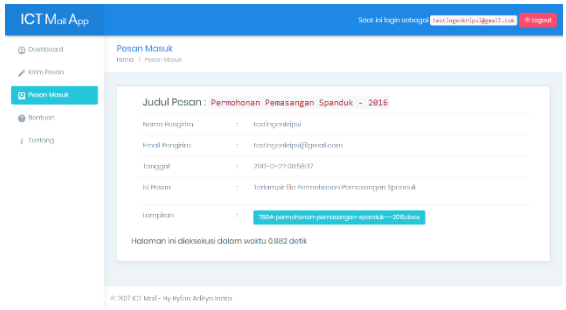


Gambar 14. Tampilan Layar Halaman Pesan Masuk

Gambar 16 merupakan Halaman untuk Lihat Pesan, yakni halaman dimana *user* telah mengklik Baca Pesan dan diarahkan ke halaman Lihat Pesan. Sebelum melihat pesan, *user* diminta untuk memasukan kunci sebagai mendekrip pesan yang dienkripsi yang dapat dilihat pada gambar 15.



Gambar 15: Tampilan Layar Halaman Masukan Kunci Dekripsi



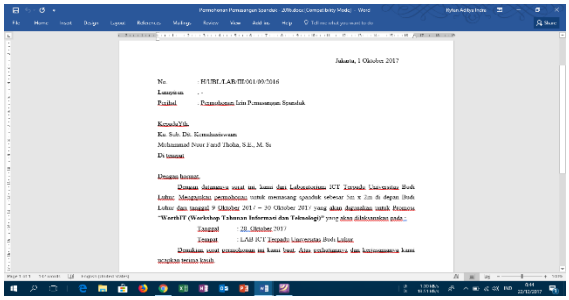
Gambar 16: Tampilan Layar Halaman Lihat Pesan

4.2. Pengujian Program

Berikut adalah pengujian program menggunakan *email Gmail*.

Judul Pesan : Permohonan Pemasangan Spanduk - 2016
Isi Pesan : Terlampir *file* Permohonan Pemasangan Spanduk

Gambar 17 merupakan lampiran *file* dengan *extension .docx*

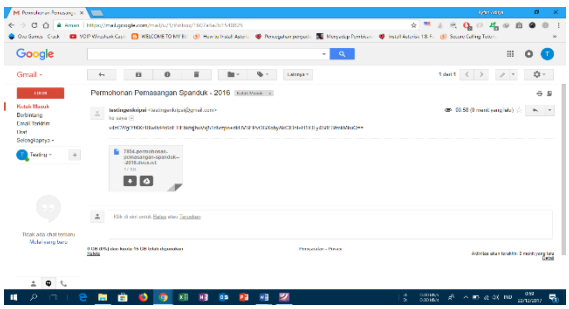


Gambar 17. Isi File Docx

Setelah pesan *email* berhasil dikirim dan dienkripsi, berikut hasilnya

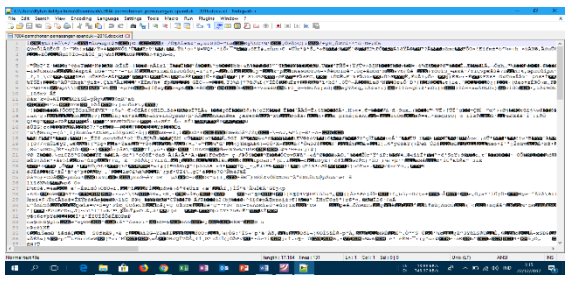
Judul Pesan : Permohonan Pemasangan Spanduk - 2016
Isi Pesan : v4zCWgIYtKKr18iwIivPc6oFTIEbktqjhuVxj51d5rzpo+dkUVSFPvOGXobyAkCIDnl+H1iOLy4S8FSfmkMkuQ==

Gambar 18 merupakan hasil enkripsi isi pesan dan lampiran yang terdapat di *Inbox Gmail*.



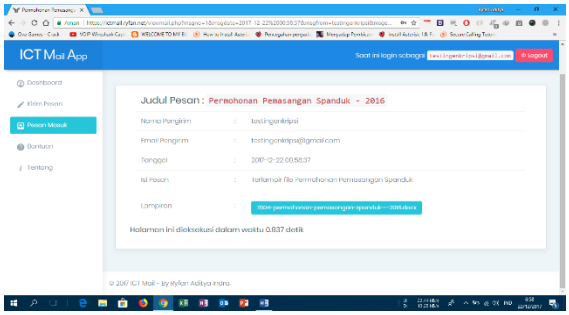
Gambar 18. Hasil Enkripsi Inbox Gmail

Gambar 19 merupakan hasil enkripsi lampiran dengan AES dan RC4



Gambar 19. Hasil Enkripsi Lampiran

Gambar 20 adalah menunjukan hasil dekripsi pesan *email* yang terenkripsi user masuk ke kotak masuk, pilih pesan yang ingin didekrip kemudian masukan kunci. Jika benar akan menghasilkan pesan utuh sesuai yang dikirim diawal.



Gambar 20. Hasil Dekripsi Pesan

5. KESIMPULAN

Adapun kesimpulan yang dapat dijabarkan berdasarkan hasil.

a. Algoritma *Advanced Encryption Standard* (AES-128) dan *Rivest Cipher 4* (RC4) dapat diimpelementasikan pada pesan *email* dalam bahasa pemrograman PHP untuk menenkripsi dan mendekripsi suatu isi pesan dan *file* lampiran.
b. Program aplikasi ICT Mail berbasis web sehingga memudahkan untuk penggunaan dan hanya memerlukan koneksi internet dan *browser*.
c. Pengimplementasian algoritma *Advanced Encryption Standard* (AES-128) dan *Rivest Cipher 4* (RC4) dikhususkan untuk mengamankan isi pesan *email* dan *file* lampiran.
d. Aplikasi ini mendukung di semua *browser* yang populer (*mostly used browser in the world*) dan sudah *support* dengan HTML5.
e. Waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi isi pesan dan *file* lampiran berbeda-beda tergantung pada jumlah karakter isi pesan, ukuran *file* lampiran dan koneksi internet.
f. Ketika mengenkripsi suatu *file* lampiran, nama *file* dan format *file* akan berubah. Nama *file* tersebut bertambah beberapa nomor unik di depan. Hal ini digunakan untuk menghindari persamaan *file* ketika mengirim.

Pada penelitian inipun terdapat saran yang bisa dijadikan pertimbangan untuk pengembangan aplikasi berdasarkan penelitian yang telah diperoleh, antara lain sebagai berikut :

a. Program aplikasi ini diharapkan dapat menambah algoritma kriptografi lainnya selain AES dan RC4 untuk meningkatkan keamanan data atau informasi.
b. Program aplikasi ini diharapkan dapat berguna bagi pengguna internet dalam pengiriman informasi dan sadar akan pentingnya suatu informasi penting di internet.
c. Program aplikasi ini dikembangkan lebih baik lagi dalam meng-*upload file* dengan ekstensi yang lainnya selain *docx, xls, pdf, rar* dan *zip*.

6. DAFTAR PUSTAKA

[1]. Bhaudhayana, G. W. and Widiartha, I. M. (2015) 'Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap', Jurnal ilmu komputer Universitas Udayana, 8(2), pp. 15–25.

[2]. Hakim, E. L., Khairil and Utami, F. H. (2014) 'Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php', Jurnal Ilmiah R & B, 10(12), pp. 1–7.

[3]. Ibrahim, A. A. (2017) 'Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)', III(1), pp. 53–60.

[4]. Nugroho, N. B., Azmi, Z. and Arif, S. N. (2016) 'Aplikasi Keamanan Email Menggunakan Algoritma Rc4', Jurnal SAINTIKOM, 15(3), pp. 81–88.

[5]. 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. doi: 2301-8488.

[6]. Putra, D. et al. (2017) 'IMPLEMENTASI ALGORITMA RC4 DAN PLAYFAIR CIPHER Permutasi Untuk S-Box', 16, pp. 328–334.