JURNAL SISTEM INFORMASI STMIK ANTAR BANGSA [Vol. XIII No. 02 AGUSTUS 2024]

Implementasi Algoritma RC6, Vigenere & DES pada Email PT Cipta Rasa Multindo

Fatmasari[1]

***Abstract*—In this digital era, information exchange is commonplace and information exchange can be in the form of text, files or other digital information. One feature that is often used to do this is e-mail or e-mail which can send and receive exchanged information quickly compared to conventional letter sending. However, sending e-mail has shortcomings in terms of security which is vulnerable to eavesdropping, fraud and other things. PT Cipta Rasa Multindo is one of the many companies that uses this e-mail feature to exchange information and quite a lot of information sent via e-mail is confidential. Therefore, it is necessary to create a method or application that can help with security in sending information via e-mail so that PT Cipta Rasa Multindo is safer in sending information, especially confidential sending.**

***Intisari*—Pada era digital ini, pertukaran informasi adalah hal yang lazim dan pertukaran informasi dapat berupa text, file maupun informasi digital lainnya. Salah satu fitur yang sering digunakan dalam melakukan hal ini adalah e-mail atau surel yang dapat mengirimkan dan menerima pertukaran informasi tersebut dengan cepat dibandingkan dengan pengiriman surat secara konvensional. Akan tetapi, pengiriman e-mail ini memiliki kekurangan dalam hal keamanannya yang rentan akan penyadapan, penipuan dan hal lainnya. PT Cipta Rasa Multindo adalah salah satu dari banyak perusahaan yang menggunakan fitur e-mail ini dalam bertukar informasi dan tidak sedikit informasi yang dikirimkan melalui e-mail terdapat hal yang bersifat rahasia. Oleh karenanya, maka perlu dibuat sebuah cara maupun aplikasi yang dapat membantu keamanan dalam pengiriman informasi melalui e-mail ini agar PT Cipta Rasa Multindo lebih aman dalam mengirimkan informasi, terutama pengiriman yang bersifat rahasia.**

***Kata Kunci*— email, kriptografi, des, vigenere, rc6**

I. PENDAHULUAN

Informasi sangatlah penting peranannya, serta bebanding lurus, dengan mudahnya informasi tersebut didapat melalui banyaknya media informasi yang sudah sangat familiar di masyarakat. Semua itu juga bisa didapat dengan mudah bahkan gratis. Oleh sebab itulah sebuah informasi menjadi sesuatu yang sangat berharga di jaman ini. Ini bisa dibuktikan jika ada sebuah informasi penting milik sebuah negara tersebar dan informasi tersebut mengenai negara lain maka bisa menyebabkan konflik antar negara. Maka dari itulah sebuah pengamanan informasi sangat penting.

Di Indonesia juga mengikuti Negara-Negara lain yakni dalam masalah perundang-undangan yang mengatur tentang penyalahgunaan media komunikasi dan informasi. Dan di Indonesia itu terdapat pada UU ITE no 28,29 pada tahun 2008 tentang penyalahgunaan informasi melalui media elektronik atau dokumen elektronik.

Dalam sistem bisnis yang telah mengacu pada komputerisasi, dimana setiap transaksi dan aktifitas bisnis sudah melalui komputer. Hal ini bisa menjadi sebuah pedang bermata dua, dimana komputerisasi akan membuat pekerjaan semakin mudah serta data yang terbukukan dengan rapi namun dengan riskannya kerusakan hardware dan kebocoran informasi menajadi sesuatu yang merugikan. Itulah yang menyebabkan hadirnya keinginan untuk membuat data serta transaksi yang kita miliki agar tidak bisa diretas orang lain atau dicuri dan disebarluaskan oleh orang lain. Untuk itulah setiap perusahaan membutuhkan keamanan komputer yang bisa menjamin tidak akan terjadi hal tersebut.

Maka hadirlah sebuah metode pendekatan yang disebut Enkripsi, dimana data yang kita miliki diatur sedemikian rupa agar hanya kita dan orang yang ingin kita berikan data tersebut yang bisa mengetahui arti dari kiriman kita yang menjadi kesepakatan antara dua belah pihak saja. Salah satu akibat jika sebuah perusahaan tidak memiliki keamanan komputer adalah kebocoran transaksi yang dilakukan. Dimana saat ini hampir semua perusahaan telah melakukan transaksi via email yang bersifat pribadi, namun hal ini tidak menutup kemungkinan terjadinya peretasan email transaksi terebut. Karena transaksi adalah sebuah alur bisnis yang sangat penting bagi sebuah prusahaan dimana kelancaran perkembangan perusahaan terletak disana memang sebuah akun pribadi yang di suport oleh beberapa vendor yang memiliki keamanan tersendiri dalam email itu, namun ini tidak bisa menjadi patokan sendiri karena masih bisa dibobol dengan beberapa cara yang sudah banyak ditemukan celahnya. Maka lebih baik menggandakan keamanan tersebut dengan keamanan yang bisa kita tau kemanaan email tersebut. Contohnya saja pada PT Cipta Rasa Multindo yang bergerak dibidang bakery ini melakukan transaksi pemesanan, pengiriman serta PO yang melalui emal akan sangat riskan jika transaksi tersebut bocor atau hilang akan membuat aktifitas bisnis perusahaan terganggu.

Pada perusahaan ini pernah terjadi sebuah human error saat melakukan pengiriman berkas transaksi dengan memasukan alamat emial tujuan yang salah dan fatalnya email salah yang dikirim itu adalah email aktif seseorang, jika orang tersebut menyebarkan berkas transaksi ini bisa menjadi sebuah masalah pada aktifitas perusahaan. Inilah kenapa dibutuhkannya pengamanan dalam aktifitas bisnis melalui email tersebut yang hanya bisa diketahui oleh perusahaan yang terkait.

[1] *Jurusan Sistem Informasi STMIK Antar Bangsa, Kawasan Bisnis CBD Ciledug, Jl. HOS Cokroaminoto No.29-35, RT.001/RW.001, Karang Tengah, Kec. Ciledug, Kota Tangerang, Banten, 15157 INDONESIA (telp:021 874561; e-mail: fsarie@gmail.com)*

A. *Masalah*

Dengan mengacu pada latar belakang tersebut, maka dapat diambil pokok permasalahan yang ada; antara lain adalah: bagaimana cara mengamankan transaksi email secara efisien dengan memanfaatkan metode kriptografi dengan menyajikannya melalui aplikasi pengiriman e-mail yang mudah digunakan.

II. LANDASAN TEORI

B. *e-Mail*

e-Mail atau yang disebut dengan surel (surat elektronik), adalah sebuah metode untuk mengirimkan pesan digital melalui internet; yang terdiri dari tujuan, isi e-mail serta penyisipan file yang dibutuhkan agar penerima dapat dengan mudah dan cepat dalam membaca informasi yang disampaikan dibandingkan dengan cara pengiriman surat secara konvensional.

Proses pengiriman e-mail ini dapat dilakukan melalui beberapa protokol; yaitu: SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3) maupun IMAP (Internet Message Access Protocol). Pada SMTP; pengiriman e-mail dilakukan melalui TCP/IP dengan port 25 melalui SMTP Client ke Server SMTP dengan melakukan pembukaan koneksi dan keberadaan Server SMTP inilah yang akan mengolah dalam pengiriman e-mail. Sedangkan pada POP3 yang dibuat pada tahun 1984 dengan konsep melakukan penarikan e-mail dari server e-mail ke aplikasi mail client pengguna yang mana caranya memiliki perumpamaan seperti kotak surat konvensional. Dan dengan POP3 ini, setelah dilakukan penarikan e-mail; maka e-mail yang ada pada server e-mail akan terhapus. Pada IMAP yang merupakan pengembangan dari POP versi 2 sebenarnya memiliki fungsi yang serupa, hanya saja perbedaan mendasarnya ada pada surat yang disimpan; dimana tidak dilakukan penyalinan dan penghapusan e-mail pada server e-mail.

C. *Kriptografi*

merupakan sebuah ilmu yang digunakan untuk penyandian data. Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "penyandian transposisi" merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan.

Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi "Caesar Cipher" yang terkenal pada jaman romawi kuno, "Playfair Cipher" yang digunakan inggris dan "ADFVGX Cipher" yang digunakan Jerman pada Perang Dunia I hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II , seperti Sigaba / M- 134 (Amerika Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jerman).

Kriptographi berasal dari kata "Crypto" yang berarti rahasia dan "graphy" yang berarti tulisan. Jadi, dapat dikatakan bahwa kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut.

William Stallings mendefinisikan Kriptografi sebagai "The Art and Science of keeping message secure". Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena merupakan sarana bagi distribusi data dan informasi. Sehingga data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan kriptografi.

Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut. Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi suatu pesan dalam bahasa sandi (ciphertext).

C = E (M),

dimana :
M = pesan asli
E = proses enkripsi
C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi) Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.
M = D (C)
D = proses dekripsi

Kriptografi yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Ada 4 syarat yang perlu dipenuhi, yaitu: Kerahasiaan: Pesan (plaintext) hanya dapat dibaca oleh pihak yang memiliki kewenangan; Autentikasi: Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain; Integritas: Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi saat dalam proses transmisi data; dan Non-Repudiation: Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirimkan.

D. *Algoritma RC6*

Dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin, algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST. RC6 dirancang untuk menghilangkan segala ketidakamanan yang ditemukan pada RC5, karena analisis pada RC5 menunjukkan bahwa ternyata jumlah rotasi yang terjadi pada RC5 tidak sepenuhnya bergantung pada data yang terdapat dalam blok.

Selain itu, serangan kriptanalisis diferensial juga ternyata dapat menembus keamanan yang ditawarkan RC5.8 RC6 juga dirancang untuk memenuhi persyaratan AES yang diantaranya adalah kemampuan untuk beroperasi pada mode blok 128 bit. Jika besar blok 128 bit langsung dipaksakan untuk diimplementasikan dengan algoritma RC5, maka akan dibutuhkan register kerja 64 bit.

Spesifikasi arsitektur dan bahasa yang menjadi tempat implementasi algoritma yang ditentukan oleh AES belum mendukung pengoperasian 64 bit yang efisien. Oleh karena itu, daripada menggunakan 2 register 64 bit seperti pada RC5, RC6 menggunakan 4 register 32 bit. Karena menggunakan 4 register maka akan terdapat 2 operasi rotasi pada setiap half-round yang ada, dan juga akan lebih banyak bit-bit yang akan digunakan untuk mempengaruhi banyaknya bit yang dirotasi.

Algoritma RC6 adalah versi yang dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b, dimana parameter w merupakan ukuran kata dalam satuan bit, r adalah bilangan bulat bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam byte.

E. Algoritma Vigenere

Vigenere cipher merupakan jenis cipher abjad majemuk yang paling sederhana. Vigenere cipher menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi.

Vigenere cipher ditemukan pertama kali oleh Giovan Battista Bellaso. Beliau menuliskan metode enkripsi yang kita kenal sebagai Vigenere cipher ini pada bukunya yang berjudul La Cifradel. Sig. Giovan Battista Bellaso pada tahun 1553. Namun, nama “Vigenere” pada Vigenere cipher diambil dari seorang yang bernama Blaise de Vigenere, yang juga merupakan penemu metode algoritma ini setelah Giovan Battista Bellaso.

Enkripsi dengan menggunakan algoritma Vigenere cipher pada dasarnya adalah menggunakan prinsip Caesar Cipher, yaitu melakukan enkripsi karakter pada plaintext menjadi karakter lain pada ciphertext. Perbedaan antara Caesar Cipher dan Vigenere cipher adalah huruf yang sama pada plaintext tidak selalu dienkripsi menjadi huruf yang sama pada ciphertext.

Hal ini terjadi karena pada Vigenere cipher, pergeseran karakternya ditentukan oleh karakter yang ada pada kata kunci dan kata ini selalu diulang. Akibatnya, karakter yang sama pada plaintext boleh jadi memiliki karakter yang berbeda pada ciphertextnya. Karena hal ini lah, Vigenere cipher merupakan cipher substitusi abjad-majemuk.

Tujuan utama dari Vigenere cipher ini adalah menyembunyikan keterhubungan antara plaintext dan ciphertext dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

F. Algoritma DES

Algoritma ini termasuk jenis simetr yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama. Yuli Andri meneliti tentang implementasi algoritma kriptografi DES pada berkas digital (M. Yuli Andri, 2009). Irjatul Wardah meneliti tentang kriptografi algoritma DES untuk image yang dikirim menggunakan telephone celuler. Indra Syahputra meneliti tentang simulasi keamanan informasi menggunakan kriptografi algoritma DES (Indra Syahputra, 2009).

William Mehuron meneliti tentang penggunaan algoritma DES dan Triple Data Encryption Algorithm (TDEA) untuk melindungi data rahasia.10 Pada penelitian-penelitian sebelumnya, penerapan algoritma DES baru menggunakan bahasa pemrograman C dan Pascal (Delphi). Adapun tujuan dari penelitian ini adalah mendesain dan membuat suatu aplikasi yang dapat melakukan penyandian (enkrip dan dekrip) menggunakan bahasa pemrograman Java. Harapannya, software tersebut dapat bermanfaat dalam mengamankan suatu informasi.

1) Algoritma Enkripsi DES

Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan didunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi Federal AS. Data plaintext dienkrip dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (internal key). DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk block cipher.

Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (external key) 64 bit. Skema global dari proses algoritma Dalam algoritma DES, terdapat kunci eksternal dan kunci internal. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci internal dapat dibangkitkan sebelum proses enkripsi ataupun bersamaan dengan proses enkripsi. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Karena ada 16 putaran, maka kunci internal yang dibutuhkan sebanyak 16 buah, yaitu K1, K2, ..., K16. Untuk mengaitkan kunci internal diperlukan beberapa langkah. Kunci eksternal 64 bit, dikompresi terlebih dahulu menjadi 54 bit menggunakan matriks permutasi kompresi PC-1. Dalam permutasi tiap bit ke-8 dari 8 byte kunci akan diabaikan. Sehingga akan ada penggunaan 8 bit dari 64 bit awal kunci eksternal.

Setelah didapatkan 56 bit hasil permutasi, selanjutnya 56 bit ini akan dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit. Lalu ke-2 bagian tersebut akan disimpan ke dalam C0 dan D0.

2) Algoritma Dekripsi DES

Pada algoritma DES proses dekripsi dan enkripsinya menggunakan kunci yang sama. Proses dekripsi pada ciphertext merupakan proses kebalikan dari proses enkripsi. Jika pada proses enkripsi urutan kunci yang digunakan adalah K1, K2, …, K16, maka untuk proses dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1. Masukkan awalnya adalah R16 dan L16 untuk deciphering. Blok R16 dan L16 diperoleh dengan mempermutasikan ciphertext dengan matriks permutasi IP-1.

G. Metode Pengumpulan Data

1) Wawancara

Metode wawancara dilakukan untuk mengumpulkan data melalui proses tanya jawab secara langsung sebagai narasumber.

2) Observasi

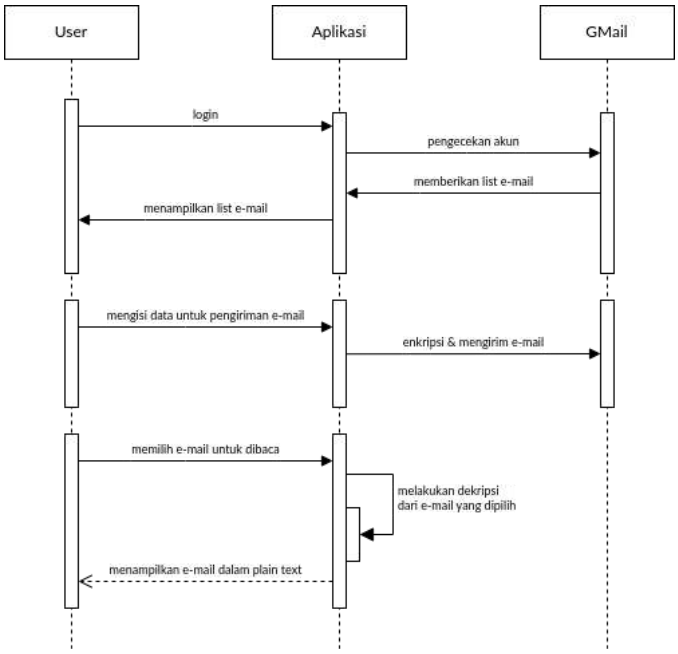
Pada metode ini, dilakukan pengamatan pada kegiatan yang berlangsung yang ada pada PT Cipta Rasa Multindo dan dilakukan penyusunan kesimpulan terhadap kebutuhan dari hasil analisa observasi ini.

3) Studi Literatur

Sebagai referensi dan sumber bahan bacaan yang terkait dengan permasalahan yang dihadapi oleh PT Cipta Rasa Multindo, maka dilakukan studi literatur yang bersumber dari beberapa buku referensi, jurnal-jurnal dan sumber dari internet yang dapat mendukung agar dapat memberikan solusi yang komprehensif atas permasalahan yang dihadapi.

H. Arsitektur Sistem

Secara garis besar, arsitektur dan flow dari proses bisnis yang dilakukan oleh aplikasi dapat dilihat pada gambar berikut ini:



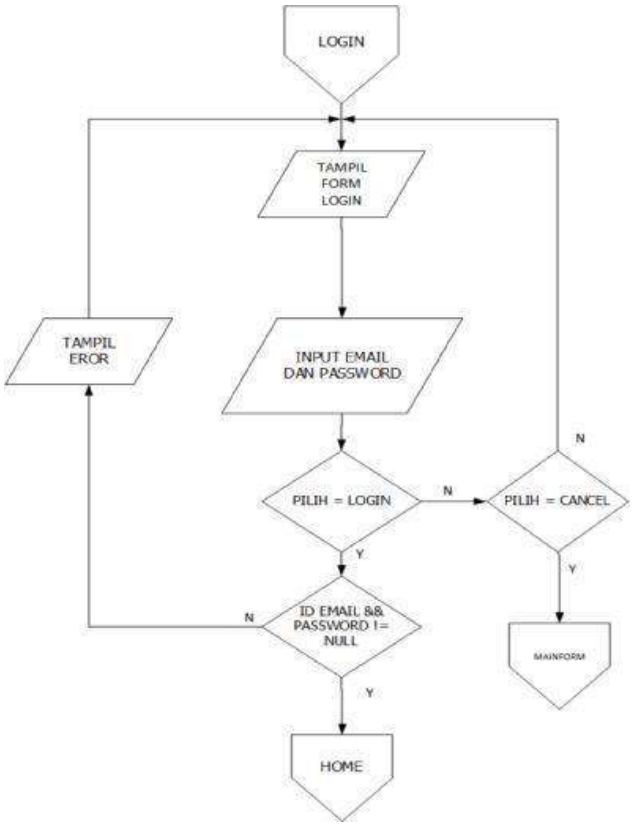
Gbr 1 Arsitektur Sistem

III. HASIL DAN PEMBAHASAN

I. Diagram Alur untuk proses login

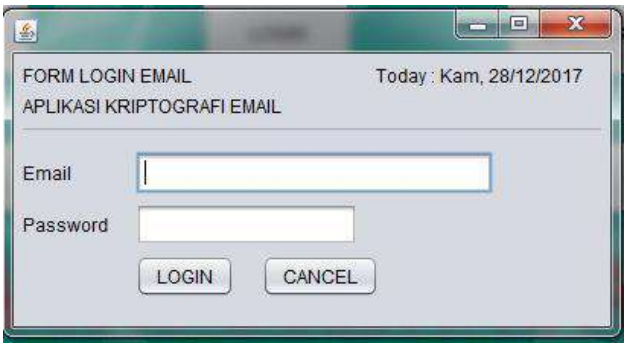
Pada flowchart ini menjelaskan tentang bagaimana user login untuk dapat menggunakan aplikasi ini. User terlebih dahulu menginput email dan password.

Jika data yang di input tidak sesuai maka akan muncul message box yang isinya menginformasikan bahwa login gagal dan user dikembalikan ke form login untuk mengisi kembali email dan password dengan benar.



Gbr 2 Diagram alur proses login

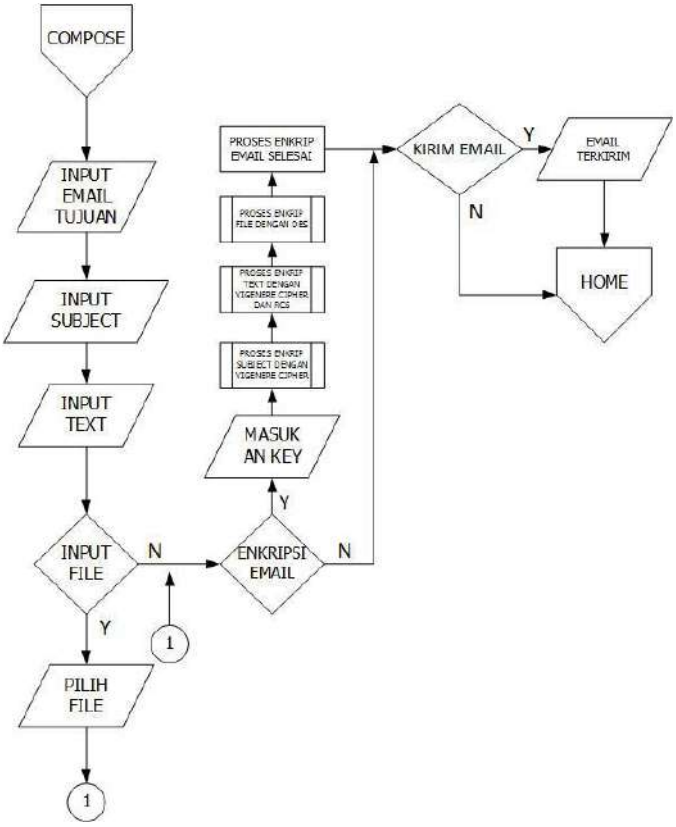
Saat user memilih menu login maka user akan dibawa ke Form login seperti yang terlihat pada gambar 4.2. Pada form ini user harus memasukan email dan password lalu mengklik tombol login untuk masuk ke menu selanjutnya.



Gbr 3 Tampilan form login

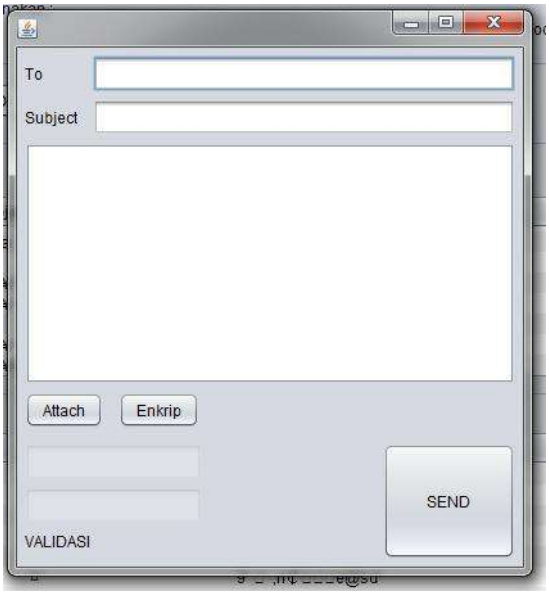
J. Diagram Alur untuk proses pengiriman e-mail

Flowchart ini menjelaskan alur dari proses mengirim pesan. Pada proses ini user dapat menuliskan isi teks email serta menyisipkan file kepada penerima. Dan juga dapat merahasiakan isi email tersebut.



Gbr 4 Diagram alur pengiriman e-mail

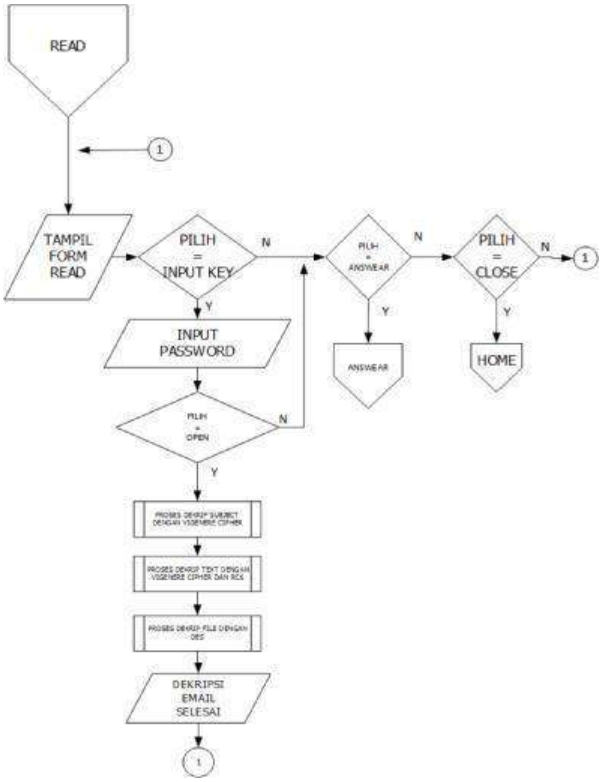
Berikut ini tampilan dari form pengiriman e-mail agar pengguna dapat mengisi tujuan, judul e-mail serta proses kriptografi yang akan diproses terhadap e-mail yang akan dikirimkan tersebut.



Gbr 5 Tampilan form pengiriman e-mail

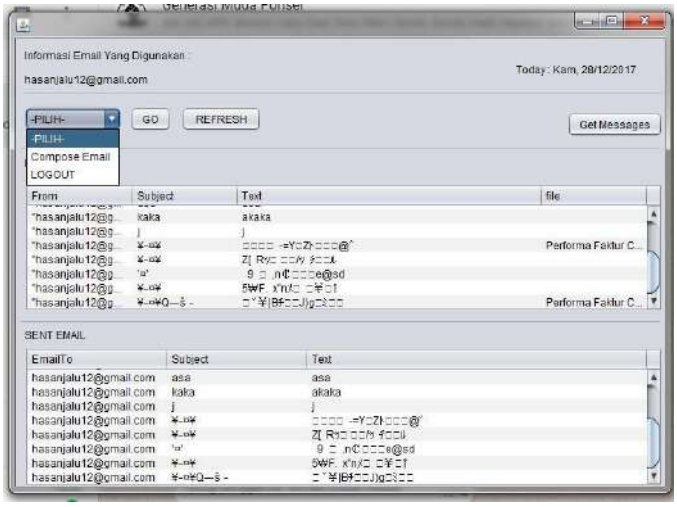
K. Diagram Alur untuk proses membaca e-mail

Pada flowchart ini menjelaskan alur proses dari membaca pesan. User harus mengklik isi email pada table inbox di menu home, setelah itu muncul form read untuk membaca isi email tersebut. Dan bisa mengembalikan isi email tersebut oleh pengirim.



Gbr 6 Diagram alur proses membaca e-mail

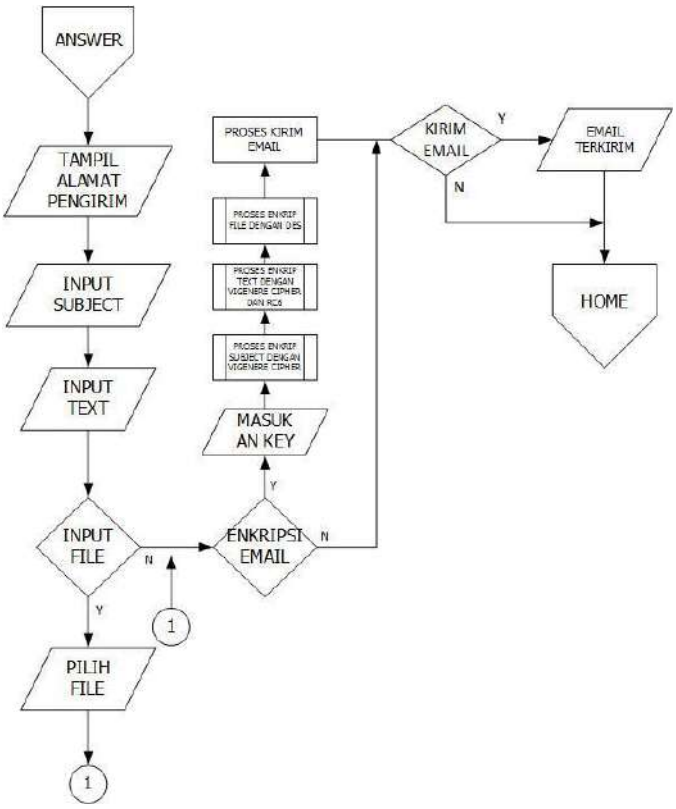
Dari diagram alur tersebut, maka pengguna akan dihadapkan pada form seperti pada gambar 7 dibawah ini; sehingga pengguna dapat memilih email mana yang akan dibaca dari daftar email yang terenkripsi tersebut.



Gbr 7 Tampilan form proses membaca e-mail

L. Diagram Alur untuk proses menjawab e-mail

Flowchart ini menjelaskan alur dari proses balas pesan. Pada proses ini user dapat menuliskan isi teks email serta menyisipkan file kepada penerima. Dan juga dapat merahasiakan isi email tersebut.



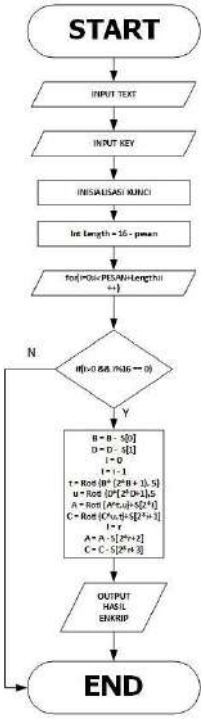
Gbr 8 Diagram alur proses menjawab e-mail

Untuk tampilan formnya, terdapat pada gambar 9 berikut ini:

Gbr 9 Tampilan form untuk menjawab e-mail

M. Diagram Alur Algoritma Enkripsi RC6

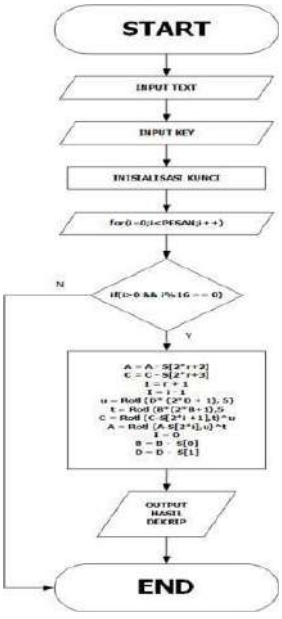
Untuk proses enkripsi algoritma RC6, dapat dilihat pada gambar 10 berikut ini:



Gbr 10 Diagram Alur Algoritma Enkripsi RC6

N. Diagram Alur Algoritma Dekripsi RC6

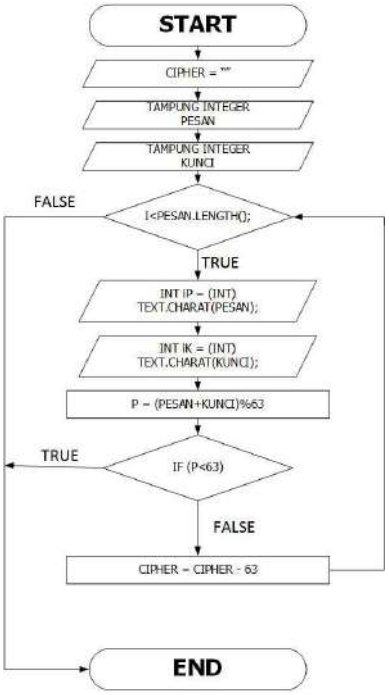
Sedangkan untuk alur dari algoritma dekripsi RC6 dijelaskan seperti pada gambar 11 berikut ini:



Gbr 11 Diagram Alur Algoritma Dekripsi RC6

O. Diagram Alur Algoritma Enkripsi Vigenere

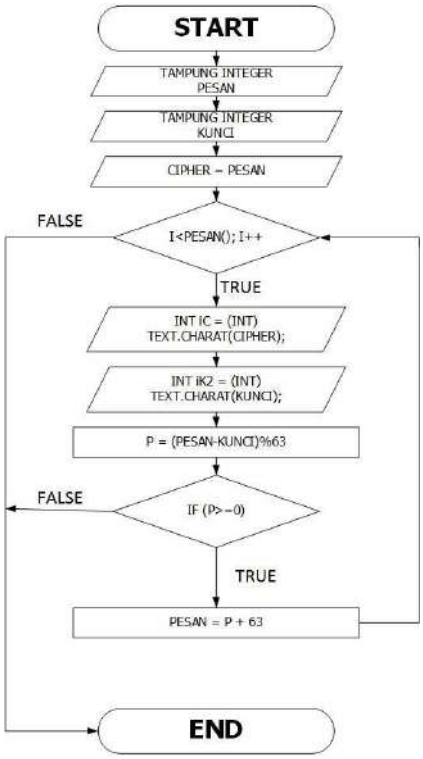
Untuk alur dari algoritma enkripsi Vigenere diterangkan seperti pada gambar 12:



Gbr 12 Diagram Alur Algoritma Enkripsi Vigenere

P. Diagram Alur Algoritma Dekripsi Vigenere

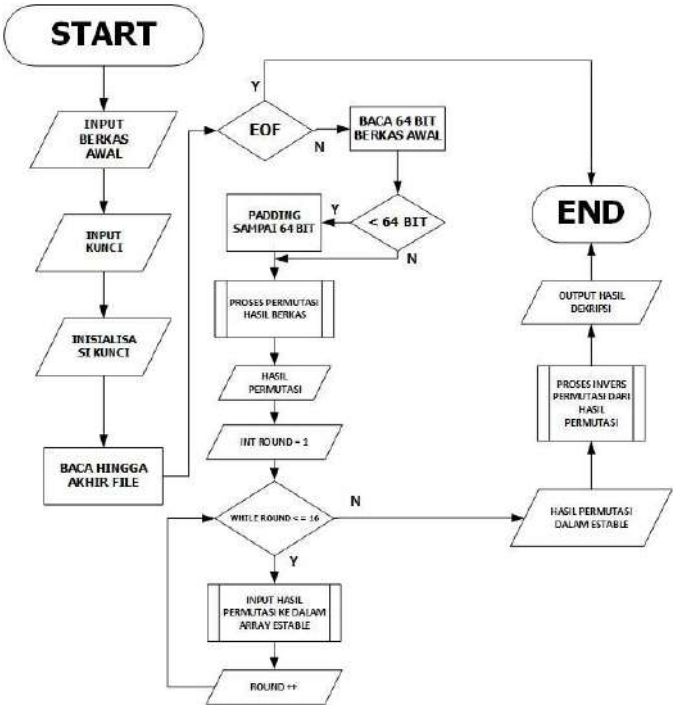
Dan untuk algoritma dekripsi Vigenere tampak pada gambar 13 ini:



Gbr 13 Diagram Alur Algoritma Dekripsi Vigenere

Q. Diagram Alur Algoritma Enkripsi DES

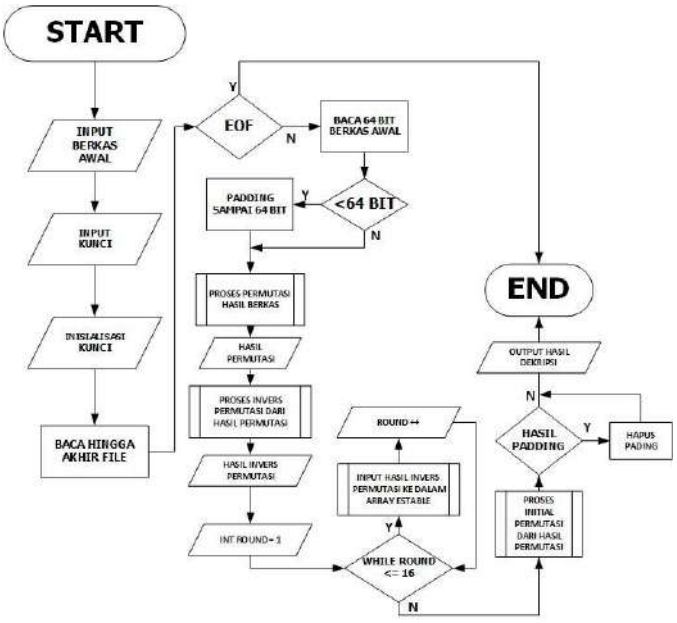
Pada aplikasi yang dikembangkan juga terdapat algoritma DES, dimana untuk alur enkripsi nya dapat dilihat pada gambar 14 berikut ini:



Gbr 14 Diagram Alur Algoritma Enkripsi DES

R. Diagram Alur Algoritma Dekripsi DES

Sedangkan untuk melakukan dekrisi dari algoritma DES tersebut dapat dilihat pada alur yang terdapat pada gambar 15:



Gbr 15 Diagram Alur Algoritma Dekripsi DES

IV. PENUTUP

Berdasarkan hasil analisa yang telah kami lakukan terhadap permasalahan dan aplikasi yang dikembangkan, maka dapat ditarik suatu kesimpulan, bahwa dengan adanya aplikasi pengamanan email ini maka setiap transaksi menjadi lebih aman dari pihak yang tidak diharuskan mengetahui transaksi tersebut; pada proses dekripsi tetap berjalan meskipun password yang dimasukan tidak sesuai, namun email dan file yang terdekripsi tidak dapat dibaca dan file tidak bisa dibuka; akan tetapi jika pada proses dekripsi dengan password yang benar akan mengembalikan email dan file menjadi email dan file semula; dan durasi yang dibutuhkan untuk melakukan enkripsi dan dekripsi berbanding lurus dengan besar kecil ukuran file yang termasuk dalam email tersebut. Selain itu, saran yang dapat dilakukan untuk pengembangan selanjutnya adalah bahwa aplikasi ini hanya dapat menyisipkan file *.doc, *.docx, *.pdf, *.xls, *.xlsx dan untuk itu kedepannya perlu dikembangkan untuk menambahkan file extension lainnya; tampilan user interface masih sangat sederhana yang kedepannya dapat menggunakan web based maupun mobile; dan dapat dikembangkan dengan menggabungkan metode kompresi sehingga ukuran file yang diproses menjadi lebih minim untuk efisiensi ruang penyimpanan ; serta durasi proses kriptografi dapat dipersingkat dalam pengembangan berikutnya.

REFERENSI

[1] Arjana, P. H. et al. (2013) 'Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper', Sentika, 2013(Sentika), pp. 164–169.
[2] Hamid (2014) 'Uji Keamanan Aplikasi Email Bawaan Android Pada Jaringan Nirkabel', Jurnal Cybermatika, 2(1), pp. 13–19.
[3] Primartha, R. et al. (2013) 'Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)', Enkrip dan Dekrip dengan DES, 3(2), pp. 371–387.
[4] Rohmanu, A. (2017) 'Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File Ajar Rohmanu', 1(2), pp. 1–11.
[5] Zulham, M., Kurniawan, H. and Rahmad, I. F. (2014) 'Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi Rc6', Seminar Nasional Informatika , pp. 96–101.

Fatmasari, S.Kom., M.Kom. lahir di Jakarta tahun 1978, lulus Strata Satu (S1) Jurusan Sistem Informasi Universitas Budi Luhur tahun 2006 dan pada tahun 2010 lulus program Pasca Sarjana (S2) Magister Ilmu Komputer Universitas Budi Luhur yang mana saat ini sebagai Dosen STMIK Antar Bangsa.