APLIKASI PENGAMANAN PESAN PADA *MAIL CLIENT* MENGGUNAKAN ALGORITMA RC6

Dede Yusuf Munandar
E-Mail: Dziewa@yahoo.com

Pembimbing I : Nana Juhana,M.T
Pembimbing II : Khusnul Novianingsih, M.Si

Jurusan Teknik Informatika, Fakultas Teknik dan Ilmu Komputer,
Universitas Komputer Indonesia

Abstrak

Dengan semakin meningkatnya pemakai komputer didunia, maka kebutuhan akan informasi semakin banyak. Karena itu pemanfaatan teknologi sangat diandalkan dan dapat menjadi penunjang pembuatan keputusan yang baik dan tepat bagi organisasi modern, baik organisasi pemerintah maupun organisasi swasta dan pemakaian teknologi informasi sudah menjadi suatu kebutuhan umum. Apalagi di dukung dengan kemajuan di bidang teknologi komputer seperti adanya jaringan komputer yang digunakan dalam komunikasi data antar sistem komputer yang makin berkembang pesat.

Berbagai macam layanan komunikasipun tersedia di internet, diantaranya *e-mail*, *millis*, *newsgroups*, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi diinternet, maka permasalahan pun bermunculan, apalagi ditambah dengan adanya *hacker* dan *cracker*. Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikanya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Dengan adanya ilmu kriptografi maka masalahpun dapat teratasi, dimana ilmu kriptografi dipakai sebagai dasar dari pembangunan aplikasi pengamanan pesan pada *mail client*.

Kata kunci: Keamanan data, E-Mail, Enkripsi

A. PENDAHULUAN

1. Latar Belakang

a. Adanya ketidakamanan dalam proses pengiriman pesan dan data
b. Adanya kebocoran pesan (message) atau penyalahgunaan pesan yang dapat berakibat fatal bagi seseorang ataupun organisasi

2. Tujuan

a. Menguji kinerja algoritma RC6 dalam mengamankan pesan
b. Menjamin keamanan pesan (message) E-mail yang dikirim dan diterima oleh seseorang dapat terlindungi dari modifikasi atau manipulasi pesan dari orang yang tidak bertanggung jawab

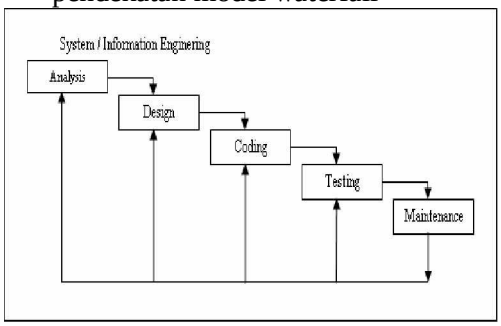
3. Batasan Masalah

a. Pengamanan pesan E-mail dengan teknik enkripsi dengan menggunakan Algoritma RC6 dan pemanfaatannya sebagai dasar dari system keamanan pengiriman pesan
b. Panjang kunci yang digunakan untuk enkripsi yaitu 128-256 bit.
c. Proses pengujian pengiriman dan penerimaan pesan hanya terbatas pada aplikasi yang dibangun.
d. Pembangunan perangkat lunak menggunakan bahasa pemrograman pascal yaitu Borland Delphi 7.0.

4. Metodologi Penelitian

a. Metode pengumpulan data

b. Metode pembuatan perangkat lunak dilakukan dengan menggunakan pendekatan model waterfall

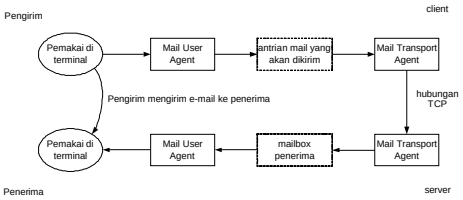


B. Landasan Teori

1. *Electronic Mail (E-Mail)*

Electronic Mail atau dapat disebut dengan E-Mail, merupakan salah satu layanan Internet yang sangat popular dan paling banyak digunakan oleh orang banyak, baik di lingkungan organisasi maupun perusahaan. E-Mail digunakan untuk saling bertukar informasi atau mengirim pesan antara seseorang dengan orang lainnya yang terpisahkan oleh jarak dan kondisi cuaca apapun dengan melewati perangkat telekomunikasi.

a. **Sistem pengiriman pesan E-Mail**



Gambar 2.1 Komponen Konseptual Sistem E-Mail

Mail User Agent (MUA) adalah perangkat lunak yang bekerja mengantarkan E-mail kepada user, sedangkan *Message Tranport Agent* (MTA). Sebagaimana dengan pengiriman pesan E-Mail kedua aplikasi ini memiliki fungsi, diantaranya yaitu fungsi dari MUA adalah sebagai berikut:

1. Menulis dan membaca pesan E-mail yang masuk baik secara *online* dan *offline* karena MUA adalah aplikasi *client* E-Mail contoh seperti: *Microsoft Outlook, Thunderbird, Eudora, Pine* dan *Pegasus*.
2. MUA dapat beroperasi tanpa perlu berkomunikasi.
3. Kemudian *user* pengguna E-mail *client* dapat melakukan penyesuaian konfigurasi E-mail sesuai dengan konfigurasi MTA yang ada pada *server mail* .

Sedangkan fungsi dari MTA adalah sebagai berikut:

1. Menentukan *header* yang digunakan untuk untuk mengenkapsulasi *teks* E-Mail, termasuk pengiriman dan penerimaan E-mail *Address.*
2. Menentukan protokol untuk mentransmisikan dan menerima E-mail
3. Menentukan protokol bagi *client* untuk memperoleh E-mail dari *server*.

b. **Protokol dan Standar E-Mail**

E-Mail memiliki protokol dan standar yang sering dipakai dalam pengiriman dan pembacaan pesan, agar pesan tersebut sampai tujuan. Standar dan Protokol utama yang digunakan dalam layanan E-mail adalah:

1. RFC 2822 atau *Internet Message Format* (IMF).
2. RFC 2821 atau *Simple Mail Transport Protocol* (SMTP).
3. RFC 1939 atau *Post Office Protocol* versi tiga (POP3).

Selain protokol POP3 yang digunakan dalam medapatkan pesan dari E-mail *server* adapun protokol yang memiliki fungsi sama yaitu *Internet Mail Access Protocol* (IMAP).

c. **Komponen E-Mail**

Secara umum Elektonik Mail terdiri atas tiga komponen yang selalu digunakan dalam pengiriman dan penerimaan pesan E-Mail, yaitu:

1. *Envelope*
2. *Header*
3. *Body*

2 Jaringan Komputer

a. Arsitektur Jaringan

Pada dasarnya, Arsitektur jaringan di bagi menjadi beberapa macam menurut fungsi dan jangkauan yang diperlukan untuk melakukan komunikasi antar perangkat, diantaranya yaitu:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Internet

b. Topologi Jaringan

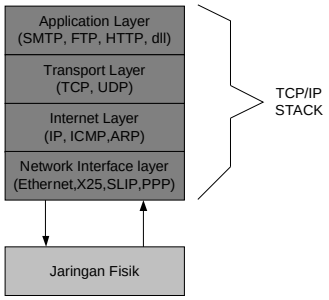
Topologi jaringan merupakan cara bagimana memperlihatkan komputer-komputer yang tersambungan di antara komputer satu dengan komputer lainnya dalam suatu jaringan. Layer jaringan harus mengikuti topologi jaringan saat ini diantaranya yaitu topologi bus, token ring, star, *peer to peer* dan *hybrid*.

c. Protokol Jaringan

Berkaitan dengan penulisan tugas akhir tentang pengamanan pesan pada E-Mail maka penulis hanya membahas protokol yang berkenaan dengan pengiriman E-Mail yaitu protokol TCP/IP.

Transport Control Protocol (TCP) berperan dalam memperbaiki pengiriman data dari *client* ke *server*. TCP dapat mendeteksi *error* atau data yang hilang dan kemudian melakukan transmisi ulang sampai data tersebut benar-benar di terima dengan lengkap.

Sedangkan *Internet Protocol* (IP) berfungsi untuk meyampaikan paket data ke alamat yang tepat dengan mendahului setiap paket data berdasarkan alamat tujuan. *Internet Authorities* menciptakan range angka untuk organisasi yang berbeda. Jadi TCP/IP adalah sekumpulan protokol yang didesain untuk melakukan fungsi–fungsi komunikasi data pada LAN, MAN, WAN. TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Sekumpulan protokol TCP/IP ini dimodelkan dengan empat layer TCP/IP



Gambar 2.2 Layer TCP/IP

TCP/IP terdiri atas empat lapis kumpulan protokol yang betingkat. Keempat lapis/layer tersebut adalah:

1. *Network Interface Layer*
2. *Internet Layer*
3. *Transport Layer*
4. *Application Layer*

3 Keamanan Jaringan Komputer

Saat ini pemakaian jaringan komputer dari *Local Area Network* sampai jaringan *Internet* bukan merupakan hal yang aneh lagi hampir semua bidang usaha dan semua informasi telah menggunakan dan dapat diakses lewat jaringan komputer, dalam kondisi yang demikian keamanan atau *security* terhadap jaringan merupakan hal yang sangat penting dan saat ini telah menjadi masalah yang menarik dan

aktual sejalan dengan pesatnya perkembangan internet dan aplikasi serta kegiatan yang ada di dalamnya, baik itu transaksi keuangan maupun transaksi informasi yang bersifat penting.

a. Aspek Keamanan Jaringan

Keamanan komputer jaringan melingkupi empat aspek utama yaitu :

- *Privacy / Confidentiality*
- *Integrity*
- *Authentication*
- *Availability*
- *Access Control*
- *Non-Repudiation*

b. Klasifikasi Keamanan Jaringan Komputer

Suatu jaringan komputer yang terdiri dari beberapa komputer yang saling terhubung satu dengan yang lainnya serta melewati beberapa titik/hub yang menghubungkan satu dengan lainnya dan dengan berbagai karakter alat serta *tool* yang digunakan menyebabkan rentannya terhadap keamanan jaringan tersebut berbagai ancaman muncul untuk menggerogoti data dan informasi yang ada, metode dan konsep pengamananpun muncul dan digunakan untuk memproteksi data dari adanya pencurian ataupun manipulasi oleh pihak - pihak yang tidak berhak dan dapat merugikan pemilik informasi tersebut, dimana konsep dan metode pengamanan tersebut dapat diklasifikasikan menjadi empat, yaitu:

- Keamanan yang Bersifat Fisik *(Physical Security)*.
- Keamanan yang Berhubungan dengan Orang *(Personel)*.
- Keamanan Data dan Media Komunikasi *(Communication)*.
- Keamanan dalam operasi.

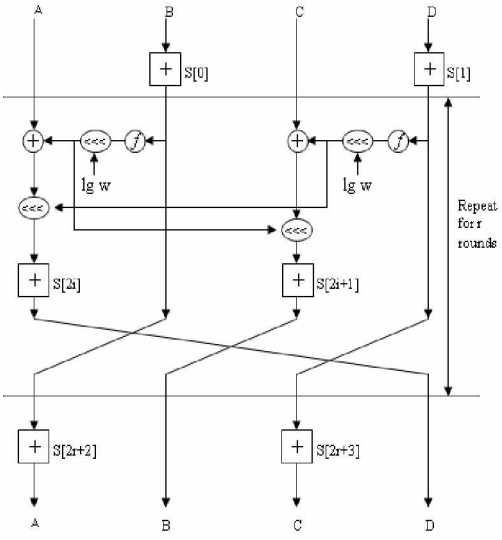
C. ANALISIS

1. Algoritma Kriptografi RC6

algoritma yang menggunakan ukuran blok 128 bit, dengan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit. Algoritma RC6 dilengkapi dengan parameter w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter r merupakan jumlah putaran / banyaknya iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte. Setelah algoritma ini masuk dalam kandidat AES, maka ditetapkan bahwa nilai w = 32, r=20 dan b bervariasi antara 16, 24 dan 32 byte.

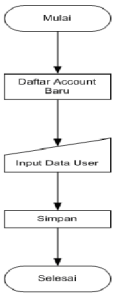
Ø Proses enkripsi

Karena RC6 memecah blok 128 bit menjadi 4 buah blok 32 bit, maka algoritma ini bekerja dengan 4 buah register 32-bit A, B, C, D. Byte yang pertama dari plaintext atau ciphertext ditempatkan pada byte A, sedangkan byte yang terakhirnya ditempatkan pada byte D. Dalam prosesnya akan didapatkan (A, B, C, D) = (B, C, D, A) yang diartikan bahwa nilai yang terletak pada sisi kanan berasal dari register disisi kiri. Diagram blok berikut akan lebih menjelaskan proses enkripsi yang terjadi pada algoritma RC6 :

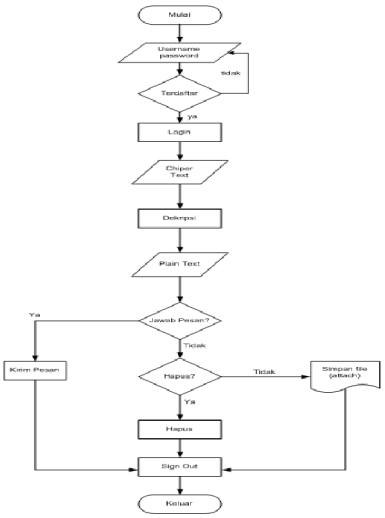


2. Perancangan system

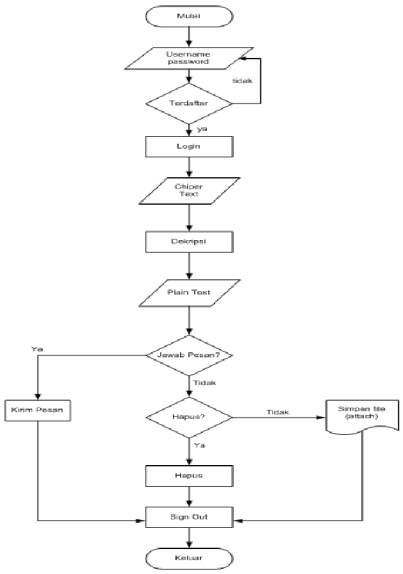
a. diagram alir proses daftar account baru



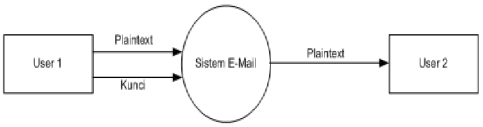
b. diagram alir proses pengiriman pesan



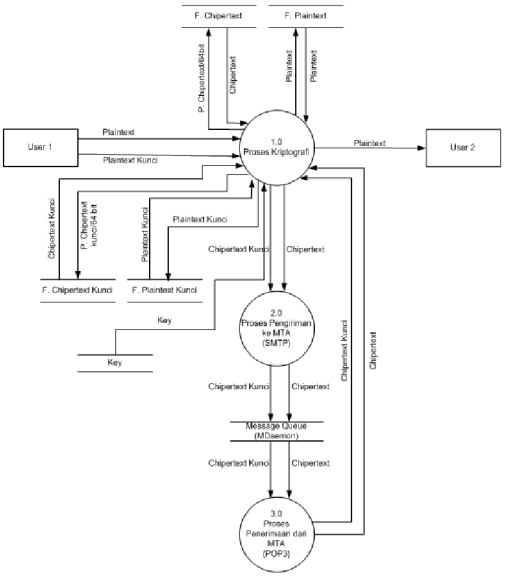
c. diagram alir poses pembacaan pesan



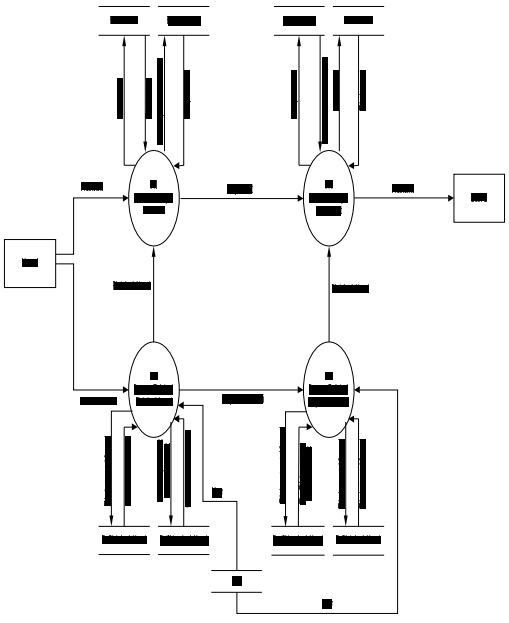
d. diagram kontek



e. Data Flow Diagram (DFD) level 0

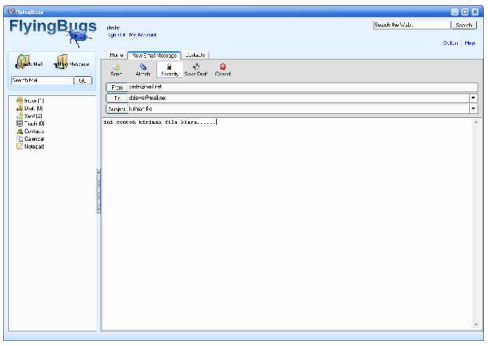


f. Data Flow Diagram (DFD) level 1 Proses 1



3. Implementasi

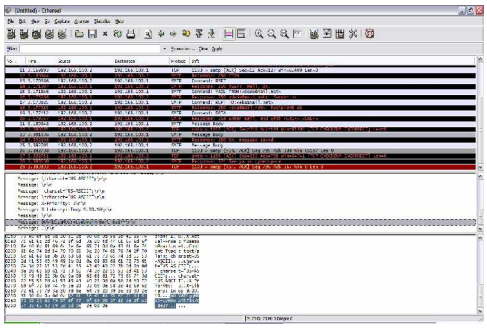
Implementasi dilakukan dengan mengetikan suatu pesan E-mail pada aplikasi yang dibangun, kemudian user diminta menggunakan fasilitas *security*, untuk mengenkripsi pesan, berikutnya *user* melakukan pengiriman. Sehingga pesan tersebut sampai ke alamat tujuan dengan hasil pesan tersebut telah terenkripsi.



Gambar Enkripsi Pesan

4. Pengujian

Pengujian kinerja aplikasi dapat dibuktikan dengan aplikasi ethereal, yaitu aplikasi yang dapat membaca setiap transmisi paket data yang lewat pada jaringan komputer. Dari hasil uji *sample* menggunakan aplikasi ethereal bahwa setiap data yang dikirim melalui aplikasi yang dibangun, dengan proses enkripsi. Pesan atau data tersebut berhasil dienkripsi dengan menunjukan pesan tersebut berubah menjadi *chiperteks* (tersandikan).



Gambar Pengujian Aplikasi Ethereal

5. Kesimpulan

Berdasarkan hasil pengujian dan analisis yang dilakukan terhadap aplikasi yang dibangun maka dapat ditarik kesimpulan bahwa :

Dari hasil uji *sample* menggunakan aplikasi Ethereal berhasil dilakukan. Bahwa pengiriman pesan menggunakan aplikasi yang dibangun, dengan melalui proses enkripsi dapat mengamankan pesan. Sehingga dengan adanya teknik enkripsi dapat dipertimbangkan menjadi salah satu solusi untuk mengamankan pesan E-mail.

6. Daftar Pustaka

1. Wikipedia (2007) Kriptografi, http://id.wikipedia.org/wiki/kriptografi/Rc6
2. *AusCERT Secure Programming Checklist*, ftp://ftp.auscert.org.au/pub/auscert/paper/security_programming_checklist/
3. Delphi3000, diakses tanggal 4 Novemeber 2007
4. http://www.delphi3000.com/category.asp?ID=40&CatName=Algorithm
5. Hariningsih, S.P., (2005), *Teknologi Informasi*,Graha Ilmu, Yogyakarta.
6. Pressman, Roger S., (2002), *Rekayasa Perangkat Lunak*, Pendekatan Praktisi Buku Satu. Andi, Yogyakarta.
7. Renaldi Munir, (2006), *Kriptografi*, Informatika, Bandung.
8. Stallings, W., (2002), *Komunikasi Data dan Komputer Jaringan Komputer*, Salemba Teknika, Jakarta.
9. Stallings, W., (2001), *Komunikasi Data dan Komputer Dasar dasar Komunikasi Data*, Salemba Teknika, Jakarta