BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Seiring dengan pertumbuhan teknologi, *e-mail* menjadi sarana komunikasi yang semakin banyak digunakan. Di negara maju, *e-mail* bahkan sudah menjadi komunikasi utama di kantor atau antara pelanggan dan nasabahnya. Pemberitahuan rapat dan segala hal yang menyangkut urusan kantor menjadi sangat praktis dengan menggunakan *e-mail*. Bahkan ada bank yang menggunakan *e-mail* sebagai komunikasi utama untuk menyampaikan tagihan kartu kredit atau komunikasi penting lainnya.

Rives't *Code* 6 (RC6) merupakan algoritma blok kode yang sangat aman, padat, sederhana dan menawarkan perfomansi yang sangat bagus dan fleksibel, dikembangkan dari algoritma Rives't *Code* 5 (RC5) oleh Ronald Linn Rivest, Ray Sidney, Matt JB, Robshaw dan Yiquin Yin dari RSA *Security*, Inc. pada tahun 1998. Ada dua fitur utama dalam RC6 dibanding RC5, yaitu perkalian integer dan penggunaan empat buah direktori berukuran w/4 bit bukan w/2 bit seperti pada RC5 (w adalah ukuran blok yang digunakan dalam satuan bit) perkalian integer

digunakan untuk menambah pencapaian *diffusion* (penyebaran yang mengakibatkan RC6 lebih aman daripada RC5) untuk tiap putaran sehingga jumlah putaran dapat diperkecil dan kecepatan proses menjadi bertambah (Ariyus, 2008).

Dengan fungsinya yang sangat penting maka sebagai pengguna harus benar-benar memperhatikan faktor keamanan *e-mail* nya. Penulisan tugas akhir ini membahas tentang faktor keamanan *e-mail* dari sisi pengguna *e-mail*, menggunakan aplikasi penyandian data dengan algoritma RC6.

1.2. Rumusan Masalah

Bagaimana membangun aplikasi untuk enkripsi dan dekripsi suatu pesan atau informasi *e-mail* sebelum dikirim atau dibuka dengan menggunakan metode algoritma RC6.

1.3. Ruang Lingkup

Sesuai dengan rumusan masalah yang ada, maka ruang lingkup untuk tugas akhir ini dibatasi pada:

1. Aplikasi tersebut dapat berjalan apabila pengirim dan penerima telah memiliki aplikasi dan kunci yang dibuat.

2. Aplikasi tersebut hanya menggunakan satu metode kriptografi yaitu metode keamanan data dengan algoritma RC6.
3. Aplikasi tersebut dapat mengirim dan menerima pesan dalam bentuk teks dan file sebanyak satu lampiran (*attachment*) yang dienkripsi.
4. Aplikasi yang akan dibuat menggunakan bahasa pemrograman Java Desktop.
5. Aplikasi tersebut menggunakan kunci simetri.
6. *Account e-mail* yang akan digunakan adalah: "*Gmail* dan *Yahoo.mail".*
7. Aplikasi tersebut hanya dapat mengenkripsi dan dekripsi data teks dan file.

1.4. Tujuan Penelitian

Dilihat dari penjelesan di atas, tujuan dari penyusunan tugas akhir ini adalah:

1. Membuat suatu aplikasi yang bisa melakukan penyandian (enkripsi dan dekripsi) terhadap sebuah pesan dan data *e-mail* sehingga ketika dikirimkan melalui jaringan yang tidak aman, isi dari *e-mail* tersebut tidak akan bisa dimengerti oleh orang yang tidak berkepentingan kecuali orang yang

mempunyai aplikasi ini dan mengetahui kunci yang digunakan untuk mengenkripsi *e-mail* tersebut.

2. Membuat aplikasi pengiriman dan penerimaan *e-mail* yang dilengkapi dengan lampiran (*attachment*).