BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan semakin pesatnya perkembangan teknologi jaringan komputer yang terintegrasi di dalam dunia telekomunikasi, khususnya jaringan global atau internet, hal ini mengakibatkan munculnya perubahan cara-cara berkomunikasi konvensional secara langsung antar individu. Di kalangan pengguna jaringan internet, terdapat banyak fasilitas aplikasi yang tersedia guna berkomunikasi user satu dengan yang lain, seperti: *instant messaging*, *interactive games* untuk ragam pemain, *video conference* dan masih banyak lainnya (H. S. Kwok, Wallace K. S. Tang dan K. F. Man, 2002:1).

Jaringan internet adalah sebuah bentuk jaringan komunikasi berskala besar antar komputer, jaringan internet merupakan sistem yang terbuka dimana segala platform sistem operasi dapat saling berkomunikasi dan informasi yang lewat di dalamnya dapat dengan mudah disadap serta diawasi. Pada umumnya, aplikasi komunikasi yang tersedia saat ini mengabaikan faktor keamanan di dalam komunikasi data. Oleh karena itu, user dihadapkan pada resiko akan terancamnya hak *privacy* atas informasi yang mereka miliki (H. S. Kwok, Wallace K. S. Tang dan K. F. Man, 2002:1).

Sebagai contoh: pihak ketiga dapat dengan mudah memonitor isi percakapan antara dua user di dalam jaringan dengan menggunakan program aplikasi bantuan (H. S. Kwok, Wallace K. S. Tang dan K. F. Man, 2002:1). Maka diperlukan suatu cara untuk mengamankan data informasi yang akan melewati

suatu jaringan komputer. Suatu metode untuk mengamankan data informasi adalah dengan menerapkan enkripsi data.

Enkripsi data merupakan teknik untuk mengkodekan sekumpulan data informasi agar tidak dapat dibaca / diterjemahkan oleh pihak yang tidak berhak atas data tersebut, dengan menerapkan enkripsi pada data informasi maka diharapkan pihak ketiga yang berkeinginan untuk memonitor data informasi antara dua user di dalam jaringan komputer tidak akan mampu membaca ataupun menterjemahkan isi dari data informasi yang didapatnya.

Salah satu solusi yang ditawarkan saat ini adalah hasil penelitian H. S. Kwok, Wallace K. S. Tang dan K. F. Man dari *Department of Electronic Engineering*, City University of Hong Kong, Kowloon yang diterima pada tanggal 28 Juni 2002 dan direvisi tanggal 4 Oktober 2002. Serta diterbitkan International Journal of Bifurcation and Chaos, Vol. 14, No. 1 (2004) 285-292.

Penelitian tersebut di atas menghasilkan sebuah aplikasi *online secure chatting* dengan menerapkan enkripsi data menggunakan algoritma *discrete chaotic map* di mana sebuah kunci digunakan untuk proses enkripsi dan dekripsi pesan. Algoritma *discrete chaotic map* termasuk dalam kategori algoritma simetrik, yaitu algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi pesan.

Berdasarkan kenyataan tersebut di atas serta penelitian yang telah dilakukan sebelumnya, maka diperlukan suatu aplikasi *secure chatting* dengan menggunakan enkripsi data dengan kemampuan yang berfungsi untuk mengamankan data informasi yang dilewatkan melalui jaringan internet dengan menggunakan algoritma yang berbeda untuk menghasilkan sebuah keamanan data

yang lebih handal serta mudah digunakan oleh user (Manish Parashar, Manish Agarwal, Steele Arbeeny, Viraj Bhat & Rangini Chowdhury. 2001 : 2).

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka permasalahan pada tugas akhir ini, adalah : " Bagaimana membuat aplikasi *secure chatting* dengan menerapkan enkripsi data sehingga data informasi yang berjalan melewati suatu jaringan tidak dapat dibaca dan dianalisa oleh pihak yang tidak berkepentingan dan menghasilkan suatu nilai tambah pada tingkat keamanan suatu jaringan ? ".

1.3 Pembatasan Masalah

Mengingat karena luasnya permasalahan dalam pembuatan tugas akhir ini, maka perlu diberikan batasan masalah dengan harapan dapat memperjelas masalah yang akan dihadapi dalam pembuatan tugas akhir ini yang meliputi :

1. Ruang lingkup rancang bangun sistem ini adalah semua komputer yang terhubung dalam suatu jaringan dan memiliki nomor Internet Protocol (I P).
2. Aplikasi yang dibuat adalah aplikasi desktop dan web based.
3. Protokol jaringan yang digunakan adalah protokol *Transmission Control Protocol/Internet Protocol* (TCP/IP).
4. Data yang akan dienkripsi merupakan data informasi text.
5. Algoritma enkripsi yang digunakan adalah RSA untuk enkripsi dengan menggunakan kunci publik dan IDEA untuk enkripsi dengan menggunakan kunci privat.
6. Bahasa pemrograman yang digunakan adalah JAVA.

1.4 Tujuan

Tujuan dari pembuatan aplikasi ini adalah membuat suatu aplikasi *chatting* yang handal dalam keamanan data sehingga dapat memberikan rasa aman pada pengguna aplikasi dalam berkomunikasi dengan pihak lain melalui jaringan komputer serta memberikan kemampuan untuk mengamankan data yang akan dikirimkan melalui jaringan komputer sehingga data informasi sulit untuk dibaca atau diterjemahkan bila disadap oleh pihak ketiga.

Aplikasi *chatting* yang dibuat dengan menggunakan algoritma RSA dan IDEA diharapkan memiliki performa yang lebih baik dalam hal kecepatan pemrosesan enkripsi maupun dekripsi data di jaringan dibandingkan dengan hasil penelitian yang telah dilakukan sebelumnya dengan menggunakan algoritma *discrete chaotic map* (Gonzalo Alvarez. 2005).

Proses enkripsi data informasi dilakukan secara *real time* dengan menggunakan dua algoritma yang berbeda dan *key* enkripsi dapat dibuat berbeda-beda antara satu user dengan yang lainnya sehingga sulit untuk diterjemahkan oleh pihak yang tidak berkepentingan.

1.5 Kontribusi

Penelitian di bidang keamanan data pada jaringan komputer terutama dalam bidang sistem pengaman data yang melalui jaringan telah banyak dilakukan dengan menggunakan berbagai macam implementasi serta metode (*Data Encryption , Steganographi)*. Dalam implementasi tugas akhir ini akan dilakukan pengembangan dari penelitian sistem keamanan data yang diintegrasikan dengan

teknik enkripsi data yang nantinya dapat melakukan proses penyandian terhadap suatu paket data berdasarkan algoritma enkripsi yang telah ditentukan.

Dalam sistem ini akan digunakan dua model aplikasi yaitu aplikasi *desktop* dan aplikasi *web based*. Adapun aplikasi yang akan dibuat menggunakan dua jenis enkripsi data yaitu menggunakan algoritma enkripsi RSA dan IDEA. Yang pertama aplikasi desktop dapat melakukan komunikasi melalui jaringan komputer.

Yang kedua memberikan kemudahan bagi user untuk berkomunikasi melalui aplikasi yang dibuat berbasis *web* sehingga user dapat lebih bebas berkomunikasi tanpa terhalang jarak. sehingga dari sistem ini diharapkan akan memberikan kontribusi penting terutama untuk kemajuan sistem keamanan data pada jaringan komputer.

1.6 Sistematika Penulisan

Laporan penelitian dan pembuatan tugas akhir ini tersusun atas beberapa bab dengan urutan sebagai berikut :

BAB I : Pendahuluan

Pada bab ini akan menguraikan mengenai latar belakang masalah, perumusan masalah, pembatasan masalah, serta tujuan yang ingin dicapai dari tugas akhir yang dibuat. Serta kontribusi yang dapat diberikan pada perkembangan sistem keamanan data pada jaringan komputer saat ini.

BAB II : Landasan Teori

Pada bab ini akan menguraikan mengenai teori-teori terkait yang berhubungan dengan variabel-variabel yang diteliti dalam pembuatan tugas akhir.

BAB III : Metode Penelitian

Pada bab ini akan menguraikan mengenai metode penelitian yang digunakan, serta alasan pemilihan metode yang digunakan dalam pembuatan tugas akhir. Serta akan memuat tentang rancangan dan implementasi dari sistem yang dibuat.

BAB IV : Pengujian dan Evaluasi Sistem

Pada bab ini akan dibahas mengenai prosedur pengujian, hasil pengujian serta analisa hasil dari percobaan yang dilakukan pada sistem yang dibuat.

BAB V : Penutup

Bab ini merupakan penutup yang berisi mengenai kesimpulan dari penelitian yang dilakukan, serta saran- saran yang bertujuan untuk pengembangan penelitian selanjutnya.