BAB I

PENDAHULUAN

1.1.Latar Belakang

Di zaman teknologi informasi ini, aplikasi *chatting* sering digunakan untuk saling tukar-menukar pesan antar pengguna komputer. Bahkan fasilitas *chatting* seakan menjadi kebutuhan sehari-hari bagi penggunanya walaupun dalam keadaan sibuk mereka tetap sempat untuk menggunakan fasilitas chatting ini karena hampir semua aspek teknologi informasi memberikan fasilitas *chatting*. Hal itu bisa di lihat dari banyaknya peminat fasilitas chatting di seluruh dunia contohnya pengguna fasilitas *yahoo messenger*, *facebook* tetapi tidak semua kalangan menggunakan fasilitas koneksi internet baik yang di rumah, kantor dan instansi – instansi pemerintah, berdasar akan hal itu maka penulis bertujuan membuat aplikasi chatting yang berbasis *LAN(Local Area Network)*, sehingga kegiatan chatting bisa berlangsung. Walaupun komunikasi yang terjadi akan berjalan secara *offline* tetap diperlukan pengamanan yang lebih karena bila saluran komunikasi yang digunakan kurang aman, maka *hacker* (penyerang) akan dengan mudah membobol saluran yang ada dan menyadap semua komunikasi yang terjadi karena hal itu dapat menyebabkan kerugian besar . Untuk mencegahnya dapat digunakan salah satu algoritma kriptografi. Sebelum data dikirim atau ditransmisikan, data terlebih dahulu disandikan dengan proses enkripsi. Dengan demikian data ditransmisikan dalam bentuk teks tersandi dan tak terbaca. Pada

keadaan ini, walaupun *hacker* dapat menyadap komunikasi, *hacker* tidak dapat mengetahui isi komunikasi yang terjadi, karena data yang berhasil disadap *hacker* adalah data dalam bentuk tersandi (terenkripsi) sehingga tidak dapat dibaca. Di tempat penerima, teks tersandi dikembalikan lagi menjadi teks semula dengan proses dekripsi. Selain fasilitas chatting pada aplikasi ini juga tersedia internet monitor yang bertujuan memonitor *browsing traffic* dari para pengguna computer yang berada di satu area network dan sedang menggunakan aplikasi chatting, fasilitas ini berfungsi lebih kepada menjaga agar para *user* tidak menyalah gunakan kemudahan mendapatkan informasi di saat sedang koneksi internet yang bisa merugikan dirinya dan orang lain.

Di dalam aplikasi *chatting & internet monitor* yang dibuat, proses koneksi antar komputer ini membutuhkan sebuah komputer yang berperan sebagai *Server* dan komputer lainnya sebagai *client*. Kehadiran *Server* sangat di butuhkan sebagai pengawas dan pengontrol dari aplikasi karena terkadang sering di dapati user yang jahil. Proses koneksi antar komputer ini dimungkinkan dengan menggunakan teknologi yang diperkenalkan *Microsoft*, yaitu *Microsoft Winsock Library*, atau lebih sering disebut dengan '*Winsock*'. Komponen ini adalah komponen *standard* VB6 dan akan ikut ter-*install* ketika komputer di-*install* dengan *software* VB6. Sedangkan algoritma kriptografi yang akan digunakan adalah algoritma WAKE. Algoritma WAKE merupakan salah satu algoritma kriptografi yang telah digunakan secara komersial. WAKE merupakan singkatan dari *Word Auto Key Encryption*. Algoritma ini ditemukan oleh David Wheeler pada tahun 1993. Algoritma ini menggunakan kunci 128 bit, dan sebuah tabel 256

x 32 bit. Dalam algoritmanya, algoritma ini menggunakan operasi XOR, AND, OR dan *Shift Right*. Algoritma WAKE ini telah digunakan pada *program* Dr. Solomon Anti Virus. Algoritma WAKE dapat dibagi menjadi beberapa proses yaitu proses pembentukan tabel dan kunci, enkripsi dan dekripsi. Proses penyelesaian algoritma ini cukup rumit dan sulit untuk dikerjakan secara manual berhubung karena algoritmanya yang cukup panjang dan kompleks.

1.2.Pokok Permasalahan

Dari apa yang telah dijabarkan dalam latar belakang masalah, maka penulis ingin mengambil rumusan permasalahan sebagai berikut:

a. Bagaimana merancang aplikasi *chatting* yang mampu mengkoneksikan beberapa komputer sekaligus di dalam jaringan *Local Area Network* (LAN) dengan menggunakan komponen *winsock*.
b. Bagaimana merancang aplikasi *internet monitor* yang mampu terhubung dengan aplikasi *chatting* agar bisa ada dalam satu bentuk aplikasi.
c. Bagaimana melakukan proses enkripsi dan dekripsi teks dengan menggunakan metode *Word Auto Key Encryption* (WAKE) dan menerapkan algoritma tersebut di dalam aplikasi *chatting* demi menjamin keamanan komunikasi.
d. Aplikasi yang di buat benar-benar mampu memuaskan keinginan para pengguna berdasarkan tingkat kepuasan mereka.

1.3.Batasan Masalah

Di dalam pembuatan tugas akhir ini, untuk mengatasi pemasalah yang ada penulis merasa perlu untuk memberikan batasan masalah yang tepat mengacu pada pokok permasalahan yang telah di rumuskan yaitu sebagai berikut :

a. Aplikasi yang dibangun, terdiri atas 2 (dua) buah aplikasi yaitu aplikasi yang berjalan sebagai *server* dan *client*, yang perlu di instalkan terlebih dahulu di beberapa komputer.
b. Fasilitas Chatting dan Internet Monitor akan berada dalam satu bentuk aplikasi dan saling berintegrasi berbasis jaringan LAN.
c. User dari aplikasi ini dibatasi hanya dapat mengkoneksikan maksimal sebanyak 50 (lima puluh) aplikasi client (*user*), agar *winsock* pada aplikasi yang akan di pakai oleh *server* tidak terlalu sibuk melayani permintaan dan pengiriman data kepada *winsock client*.
d. Aplikasi yang di pakai sebagai *server* harus mendapat perhatian penuh sehingga dapat mengeluarkan salah satu *user/client* (*kick*) jika terdapat user penganggu.
e. Sekuritas kriptografi WAKE diatur pada seluruh aplikasi chatting yang sedang berjalan di beberapa computer yang telah di instalkan aplikasi chatting ini terlebih dahulu.

   Pengaturannya adalah sebagai berikut :

   1. Kunci proses enkripsi dan dekripsi, dibatasi sebanyak 16 karakter (sesuai dengan metode WAKE).

2. Putaran pada proses pembentukan kunci yang digunakan adalah sebanyak 5 putaran.
3. *Output* dari hasil enkripsi dihasilkan dalam bentuk heksa, sedangkan *output* dari hasil dekripsi dihasilkan dalam bentuk *ascii*.

f. Aplikasi akan menampilkan user – user yang aktif.
g. Panjang tiap pesan (untuk 1 kali kirim) dibatasi sebanyak 100 karakter.
h. Perangkat lunak dibangun dengan menggunakan bahasa pemograman *Microsoft Visual Basic* 6.0.

1.4.Maksud dan Tujuan Penelitian

Maksud dari penelitian ialah demi menunjang kebutuhan data, informasi dalam penulisan skripsi ini dan bagaimana menerapkan metode *WAKE* (*Word Auto Key Encryption*) pada aplikasi chatting, mempelajari pemakaian konektifitas yang diberikan oleh winsock pada Visual Basic sehingga dapat mengimplementasikannya dengan membuat aplikasi chatting, dan sebagai syarat untuk menyelesaikan pendidikan program Sarjana (S1) Jurusan Sistem Informasi pada Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta. Adapun tujuan yang hendak dicapai dari penelitian ini adalah:

1. Menerapkan metode kriptografi *Word Auto Key Encryption* (WAKE) di dalam aplikasi *chatting* untuk menjamin keamanan komunikasi.
2. Menghasilkan suatu perangkat lunak aplikasi *chatting & Internet Monitor* berbasis jaringan LAN.

1.5.Metode Penelitian

Untuk melengkapi kelancaran dalam pembuatan skripsi ini digunakan data serta literature dan sumber – sumber yang mendukung sesuai dengan maksud dan tujuan penyusun skripsi. Adapun metode yang diterapkan dalam melakukan penelitian untuk pengumpulan data adalah sebagai berikut :

1. Metode Wawancara

   Dengan mengajukan pertanyaan langsung kepada pengguna fasilitas – fasilitas chating dengan berlandaskan pada tujuan penelitian dan objek yang diteliti.

2. Studi Pustaka

   Studi pustaka ini mengacu pada buku-buku pedoman yang dibutuhkan baik yang ada diperpustakaan, maupun literatur-literatur yang berhubungan dengan masalah yang diteliti sehingga nantinya dapat membantu selesainya skripsi ini.

3. Perancangan

   Tahap ini merupakan perancangan dari model permasalahan yang ada. Pada tahap ini dihasilkan rancangan komponen-komponen aplikasi yang akan di buat

4. Pengkodean

   Menerjemahkan hasil proses perancangan menjadi sebuah bentuk program komputer yang dimengerti oleh mesin komputer. Tahap ini merupakan perancangan dari model permasalahan yang ada.

5. Pengujian

   Meliputi pengujian unit aplikasi dan pengujian aplikasi secara keseluruhan.

1.6.Sistematika Penulisan

Sistematika penulisan skripsi ini dapat dipaparkan secara singkat sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini akan diuraikan mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat, metode pengumpulan, sistematika penulisan.

BAB II DASAR TEORI

Dalam bab ini akan diuraikan mengenai konsep dasar metode kriptografi yang akan di pakai dalam aplikasi tersebut,serta dasar teori perangkat lunak (software yang digunakan).

BAB III PERANCANGAN SISTEM

Pada bab ini akan memaparkan tentang analisis chatting secara umum, analisis implementasi kriptografi pada aplikasi dan sistem pendukung, serta perancangan Aplikasi secara umum,dan pemodelan yang dipakai pada tahap perancangan aplikasi.

BAB IV IMPLEMENTASI SISTEM

Pada bab ini berisikan tentang hasil, uraian pembahasan spesifikasi proses dan prosedur pelaksanaan program yang telah di buat.

BAB V PENUTUP

Merupakan bab penutup yang berisi kesimpulan-kesimpulan dari proses pembuatan aplikasi dan berupa saran untuk perbaikan aplikasi yang dihasilkan untuk masa akan datang

DAFTAR PUSTAKA

Bagian ini memuat keterangan dari buku-buku dan literature lain yang menjadi acuan dalam penyusunan skripsi ini.