I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia telekomunikasi di dunia berkembang pesat seiring dengan semakin banyaknya penggunaan fasilitas internet di hampir seluruh lapisan masyarakat dunia. Tidak dapat dipungkiri internet ikut memberikan andil yang besar dalam perkembangan komunikasi jarak jauh.

Berbagai macam model alat komunikasi dapat dijumpai, baik yang berupa fisik (*hardware*) atau berupa aplikasi (*software*). Aplikasi yang paling sering digunakan untuk bertukar informasi adalah aplikasi *chatting*. Dengan aplikasi ini, pengguna bisa terhubung dengan siapa saja di belahan bumi hanya dengan bermodalkan akses internet. Banyak pengembang melihat kesempatan ini, oleh karena itu dapat dijumpai banyak sekali aplikasi *chatting* berbagai model dengan fitur-fitur dan penggunaan teknologi terbaru yang dikembangkan.

Namun, tidak semua perkembangan teknologi komunikasi ini memberikan dampak yang menguntungkan bagi dunia komunikasi. Penyadapan data

merupakan hal yang paling ditakuti oleh pengguna jaringan komunikasi pada saat ini.

Dengan adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*).(Raharjo, 2005)

Enkripsi dilakukan dengan kunci (*key*). Jenis dari kunci untuk enskripsi ada dua macam, yaitu kunci simetris (*symmetric/private key*) dan kunci asimetris (*asymmetric/public key*). Beberapa metode kunci simetri di antaranya adalah DES (*Data Encryption Standard*), Triple DES (3DES), IDEA (*International Data Encryption Algorithm*), Blowfish, Gost, Safer, LOKI, FEAL, RC2, RC5, Serpent. Salah satu algoritma kriptografi yang terbaru adalah algoritma Rijndael.

Algoritma Rijndael adalah pemenang sayembara terbuka yang diadakan oleh NIST (*National Institute of Standards and Technology*) untuk membuat standard algoritma kriptografi yang baru sebagai pengganti *Data Encryption Standard* (DES). DES sudah dianggap tidak aman, terutama karena panjang kunci yang relatif pendek sehingga mudah dipecahkan menggunakan teknologi saat ini. Standard tersebut diberi nama *Advanced Encryption Standard* (AES). Tepatnya pada bulan November 2001, algoritma Rijndael ditetapkan sebagai AES, dan diharapkan Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka permasalahan yang dapat diambil dari penelitian ini adalah :

1. Bagaimana membuat pesan yang dikirim pada *chatting* menjadi lebih aman.
2. Bagaimana bentuk implementasi metode kriptografi Rijndael yang diterapkan di aplikasi *chatting* pada jaringan *Local Area Network*.

1.3 Batasan Masalah

Untuk lebih memfokuskan terhadap permasalahan, maka dalam hal ini perlu batasan-batasan terhadap permasalahan yang diteliti, yaitu sebagai berikut:

1. Algoritma yang digunakan adalah Algoritma Rijndael yang dijadikan *Advanced Encryption Standard* (AES), dengan ukuran blok 128 bit dan ukuran kunci sebesar 128 bit.
2. Aplikasi yang dirancang dikhususkan pada *conference chat*
3. Bahasa permrograman yang digunakan untuk membangun aplikasi ini adalah Visual Basic (VB) 6.
4. Pesan yang dikirim atau yang diterima berupa teks.
5. Aplikasi yang dibangun tidak menangani proses pendistribusian kunci.
6. Komunikasi *chatting* dilakukan pada jaringan LAN.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mempelajari algoritma Rijndael agar dapat disesuaikan dan digunakan pada aplikasi *chatting* yang dibangun.
2. Membuat perangkat lunak *chatting* dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan dekripsikan pesan yang dikirim/diterima.

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dalam penelitian ini adalah

1. Memberikan pengamanan terhadap pesan yang dianggap penting supaya tidak dapat dilihat oleh orang yang tidak diizinkan terhadap akses pesan tersebut.
2. Memberikan kenyamanan dalam ber-*chatting*, sebab pesan yg dikirim telah terenkripsi terlebih dahulu.