BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertukaran pesan (*chatting)* sudah luas digunakan oleh berbagai kalangan. Pesan yang dikirimkan sering berisi informasi yang penting. Masalah keamanan informasi pesan (*chatting)* seringkali kurang mendapat perhatian dari perancang dan pengelola informasi. Pesan (*chatting)* tidak akan menjadi rahasia lagi apabila ditengah jalan informasi itu diakses oleh orang yang tidak berhak atau tidak berkepentingan.

Pada proses pengiriman pesan (*chatting*) terdapat beberapa hal yang harus diperhatikan, yaitu : kerahasiaan, integritas data, autentikasi dan *non repudiasi*. Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean data sebelum dilakukan proses pengiriman. Sehingga pesan (*chatting*) yang dikirim terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas data tersebut.

Untuk menjaga kerahasiaan, salah satunya dengan enkripsi data informasi yang akan dikirimkan dengan kriptografi. Enkripsi data yang bisa dilakukan menggunakan algoritma RSA(Rivest-Shamir-Adleman). Algoritma RSA (Rivest-Shamir-Adleman) digunakan untuk membangkitkan sebuah kunci rahasia antara dua komputer yang saling terhubung. RSA (Rivest-Shamir-Adleman) digunakan dengan alasan tingkat keamanan sangat tinggi.

Dalam tugas akhir ini akan dilakukan implementasi algoritma RSA (Rivest-Shamir-Adleman) dalam pertukaran pesan antara dua komputer yang terhubung jaringan. Sehingga komunikasi antara komputer yang terhubung jaringan bisa terjamin keamanannya.

1.2 Rumusan Masalah

Permasalahan yang diangkat dalam menyelesaikan tugas akhir ini adalah bagaimana mengimplementasikan algoritma RSA (Rivest-Shamir-Adleman) pada

layanan *chatting* berbasis LAN *(Local Area Network)* sebagai solusi untuk mengamankan pesan yang dikirimkan.

1.3 Batasan Masalah

Masalah dalam tugas akhir ini dibatasi oleh beberapa hal berikut:

1. Perangkat lunak akan menampilkan proses enkripsi dan deskripsi dari pesan tersebut secara singkat.
2. Perangkat Lunak dijalankan dengan 2 client
3. Enkripsi dan Deskripsi pesan dilakukan dengan menggunakan algoritma RSA (Rivest-Shamir-Adleman).
4. Aplikasi pesan akan dijalankan dengan jaringan LAN *(Local Area Network)*
5. Aplikasi dijalankan dalam bahasa pemrograman PHP dengan web server XAMPP

1.4 Tujuan

Tujuan penyusunan tugas akhir (skripsi) ini adalah

1. Mengimplementasikan algoritma RSA (Rivest-Shamir-Adleman).
2. Mengamankan dan merahasiakan pesan dalam jaringan dengan mengimplementasikan algoritma RSA (Rivest-Shamir-Adleman).

1.5 Manfaat

Manfaat dari penyusunan tugas akhir (skripsi) ini, yaitu :

1. Merahasiakan percakapan dengan media jaringan dari orang yang tidak berkepentingan
2. Membantu pemahaman tentang implementasi algoritma RSA (Rivest-Shamir-Adleman) dalam jaringan LAN (*Local Area Network*)