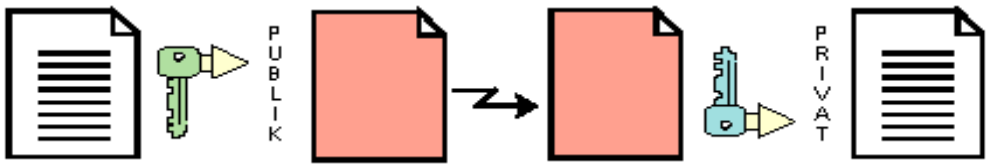
BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dewasa ini meningkat semakin pesat. Semakin mudah penggunaan sistem informasi, semakin muncul kekhawatiran akan keamanan dari data yang kita miliki pada sistem tersebut. Untuk meningkatkan keamanan pada alur transfer data yang dilakukan, maka diperlukan sebuah gembok untuk mengunci data tersebut. Dan hanya yang dapat membuka data tersebut hanyalah pihak yang bersangkutan.

Kriptografi merupakan pilihan yang tepat dalam pengaman semacam ini.Algoritma kriptografi dibagi menjadi dua yaitu, algoritma simetris dan asimetris.Kriptografi simetris hanya memakai satu kunci dalam proses enkripsi dan dekripsi. Tingkat kompleksitas algoritma ini tidak terlalu tinggi, atau bisa dikatakan ringan.Kriptografi asimetrik hanya memiliki 1 kunci public enkripsi, tetapi hanya yang memiliki kunci private yang dapat mendekripsi pesan. Jadi tingkat keamanan lebih tinggi dibandingkan kritografi simetris, tetapi tingkat kompleksitas algoritmanya lebih tinggi. Alur dari kriptografi asimetris dapat dilihat pada gambar 1.1



Gambar 1. 1 alur umum kriptografi asimetris

Keterangan

- Dokumen atau plain text (kertas putih) dienkripsi dengan kunci publik dihasilkanlah chipper (kertas merah)
- Chipper dikirim.
- Chipper diterima dan didekripsi menggunakan kunci privat maka dihasilkan dokumen asli.

Algoritma kriptografi *RSA*dianggap dapat memenuhi tingkat sekuriti yang tinggi. Dengan kombinasi hasil kali 2 bilangan prima, akan sulit untuk ditemukan dan akan memakan waktu yang sangat lama jika menggunakan *bruteforce.*Kunci RSA dengan panjang 1024bit akan menghabiskan waktu 1.43×10^{213} tahun. Waktu yang diperlukan melebihi perkiraan umur alam semesta yang dikalkulasi hanya sekitar 13.75×10^{9} tahun.

Aplikasi Chatting sudah banyak dipakai untuk berkomunikasi cepat dan instan. Banyak kalangan telah menggunakan aplikasi chatting tersebut. Semakin mudahnya alur komunikasi yang dilakukan, makin dikhawatirkan masalah keamanan pada pesan yang akan dikirim satu sama lain. Sebagai contoh, kalangan

enterprise biasa menggunakan aplikasi *chatting* dalam berkomunikasi pada rapat penting atau interaksi antar sesama karyawan. Misalkan sebuah perusaan besar Microsoft sedang mempublikasikan produk baru yang akan mereka rancang kesemua karyawan tanpa bantuan *secure chat,* maka dengan mudah ide tersebut dapat disadap kompetitor dan segera membuat produk serupa dengan yang akan dirancang oleh Microsoft tadi. Maka dengan menggunakan enkripsi pada pesan yang akan dikirim maka pesan tersebut akan aman sampai pada tujuan. Walaupun pesan tersebut telah disadap ditengah jalan, akan tetapi akan membutuhkan waktu untuk melakukan *bruteforce* pada hasil sadapan tadi dan akan memakan waktu yang sangat lama. Makan pesan tersebut dapat aman sampai tujuan tanpa diketahui pihak lain yang tidak bertanggung jawab.

Tugas akhir ini melakukan implementasi RSApada *client-serverbased Chat*. Aplikasi yang dibuat adalah 1 aplikasi *server* dan 1 aplikasi *client* yang telah dilengkapi dengan fitur enkrpsi pada pesan yang akan dikirim. Setiap pemrosesan enkripsi dan dekripsi akan dianalisa kinerjanya per *user* dan akan dihitung tingkat kenyamanan per *user* dalam penggunaan aplikasi tersebut.

1.2 Tujuan dan Manfaat

Tujuan dan manfaat dari tugas akhir tentang pengaplikasian algoritma kriptografi *RSA* pada aplikasi *chatting* ini adalah sebagai berikut :

1. Menganalisa alur data pada protokol.
2. Menerapkan algortima RSA pada *Client Chat.*
3. Menghitung performansi *Client Chat* setiap percobaan.

1.3 Rumusan Masalah

Adapun rumusan masalah pada tugas akhir ini antara lain :

1. Bagaimana Menganalisa alur data pada protokol?
2. Bagaimana proses enkripsi dan dekripsi dari kriptografi *RSA*?
3. Bagaimana penerapan RSA pada *Client Chat*?
4. Bagaimana performansi dari *Client Chat* setiap percobaan?

1.4 Batasan Masalah

Agar pembahasan tidak menyimpang dan meluas, maka masalah akan dibatasi sebagai berikut :

1. Kriptografi asimetris yang digunakan adalah algoritma RSA.
2. Berbasis *Client-Server Chat* dengan maksimal *Client* adalah 2.
3. Proses enkripsi dan dekripsi dijalankan pada CPU*Client*.
4. Tidak dilakukan proses *brute-force.*

1.5 Metologi

Metode pendekatan yang digunakan pada tugas akhir ini adalah

1. Study literature

Mencari buku pedoman atau e-*book* yang berkaitan dengan yang akan dirancang pada tugas akhir ini, juga sebagai dasar teori BAB II.

2. Perancangan Algoritma

   Melakukan percobaan penerapan pada *Client Chat*dan dihitung kecepatan pada enkripsi dan dekripsi

3. Analisis

   Melakukan analisa performansi dari segi waktu dan *resource* memori yang dipakai. Melakukan simulasi penyadapan pada setiap percobaan yang dilakukan oleh *user*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun sesuai dengan rencana berikut :

BAB I Pendahuluan

Bab ini menjelaskan latar belakang, tujuan dan manfaat, rumusan masalah, batasan masalah, metodelogi penelitian, dan sistematika penulisan tugas akhir.

BAB II Dasar Teori

Bab ini menjelaskan teori dasar yang mendukung dalam perancangan program *EncryptedClient-Server chat*.

BAB III Rancangan Sistem

Bab ini menjelaskan bagaimana membangun sistem berdasarkan kebutuhan general, dan menjelaskan detail UML diagramnya.

BAB IV Analisis Hasil Implementasi

Bab ini menjelaskan performansi algoritma RSA dan skenario program yang dilakukan oleh masing-masing user.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan yang dapat ditarik dari perancangan sistem dan scenario yang telah dilakukan serta saran bagi para pembaca untuk pengembangan tugas akhir ini.