Implementasi dan unjuk kinerja 1024 bit RSA dan diffie-Hellman

Ariefiazif, author

Abstrak

Saat ini penggunaan koneksi sudah semakin meluas, mulai dari kalangan pribadi hingga kalangan bisnis dan pemerintahan. Seringkali pengguna ingin agar informasi yang dikirim hanya bisa dibaca oleh pihak penerima saja. Hal ini dapat diwujudkan dengan menggunakan proses enkripsi. Proses enkripsi umumnya menggunakan sebuah kunci unik yang dipergunakan untuk menyandikan informasi yang dikirim, sehingga tanpa kunci yang lepat pihak penerima tidak bisa membaca informasi yang telah terenkripsi Permasalahan terdapat pada proses pengiriman kunci tersebut, bagaimana agar kunci lersebut dapat dikirim ke pihak yang dituju tanpa dapat disadap oleh pihak lain.

Untuk mengatasi permasalahan itu digunakan Public Key Cryptography (PKC). pada PKC setiap informasi yang telah terenkripsi memiliki dua kunci, kunci pribadi dan kunci publik. Kunci publik digunakan untuk mengenkripsi informasi dan diberikan ke setiap pengguna, sedangkan kunci pribadi disimpan secara rahasia dan digunakan untuk mendekript informasi yang dikirim, dan tidaklah memungkinkan pada saat ini untuk mendapatkan kunci pribadi berdasarkan dari kunci publik apabila panjang kunci publik yang dibcrikan mencapai 1024 bit [1].

Pada skripsi ini dibuat perangkat lunak dengan menggunakan bahasa Visual C++. Dari perangkat lunak yang dibuat kemudian akan dilakukan uji coba dan perbandingan kecepatan antara dua algoritma PKC yang berbeda, RSA dan Diffie-Hellman. Proses pengiriman kunci dengan menggunakan PKC ini dapat mengatasi pemlasalahan pengiriman kunci antara dua pihak, tetapi masih memiliki kelemahan terhadap mem in the middle attack. Selain itu apabila kunci publik yang digunakan lebih kurang dari 512 bit [1], maka proses pengiriman kunci tersebut tidaklah aman.