ABSTRAK

Mode transisi IPv6 ke IPv4 adalah salah satu solusi untuk melakukan perubahan IPv4 ke IPv6, salah satu modenya adalah 6to4. Namun ada pertimbangan keamanan dalam menggunakan 6to4 yaitu setiap router 6to4 harus menerima dan meneruskan paket dari *native* IPv6 maupun dari router 6to4 lainnya. Sehingga, mode transisi IPv6 ke IPv4 yang digunakan pada jaringan public mungkin meninggalkan celah karena karena tidak adanya deteksi terhadap suatu serangan seperti *sniffing,* dan *spoffing*.

Dalam keamanan jaringan dikenal berbagai algoritma untuk melakukan enkripsi dan dekripsi pesan, salah satunya adalah RSA (Rivest Shamir Adleman). Algoritma RSA merupakan algoritma kriptografi *asimetry,*dimana kunci enkripsi tidak sama dengan kunci dekripsinya. RSA masih digunakan secara luas dalam protokol *electronic commerce*, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang. Dan untuk memecahkan kunci yang cukup panjang tersebut, memerlukan waktu yang cukup lama. Dalam Tugas Akhir ini dianalisa bagaimana penggunaan algoritma RSA untuk mengamankan data dan komunikasi antara *client* dan *server* pada jaringan 6to4 yang masih rentan terhadap pencurian data.

Dari hasil analisa yang dilakukan, saat mengirimkan data sebesar 10 MB *delay* SSH *server* adalah 64,1172 ms sedangkan *delay* FTP *server* adalah 39,6879 ms. Namun, keamanan data teks yang dilewatkan pada SSH masih lebih baik dari FTP karena pada saat melakukan *long* ke *server* SSH, *password, username,* dan isi data sudah terenkripsi. berbeda halnya ketika menggunakan FTP, semua komunikasi dapat diketahui (di-*sniffing*) oleh *attacker*. Selain itu dengan adanya enkripsi dengan algoritma RSA menyebabkan utilitas CPU menjadi lebih besar yaitu 15,19355 % pada SSH *server,* sedangkan 1,333333 % pada FTP *server* (tanpa enkripsi).

Kata kunci : **spoofing, sniffing, RSA, delay .**