ABSTRAK

VPN (*Virtual Private Network*) merupakan suatu cara untuk membuat sebuah jaringan bersifat *private* dan aman dengan menggunakan jaringan publik misalnya *internet*. Jaringan publik yang digunakan saat ini sangat rentan terhadap ancaman keamanan seperti pencurian data, dan memberikan kerugian yang besar apabila data yang dicuri adalah data penting transaksi bisnis suatu perusahaan. Oleh karena itu, dibutuhkan jaringan yang tidak bisa diakses oleh publik. Data yang dilewatkan dienkapsulasi terlebih dahulu kemudian dienkripsi agar tidak terbaca ketika melewati jaringan publik karena harus melewati proses dekripsi.

Dikenal tiga jenis VPN dalam implementasinya, yaitu *trusted, secure*, dan *hybrid* VPN [18]. *Secure* VPN adalah perpaduan teknologi *tunneling* dan enkripsi. Penggunaan enkripsi dalam teknologi VPN membuat VPN tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan karena harus melewati proses dekripsi terlebih dahulu.

Implementasi jaringan VPN berbasis IPSec (*Internet Protocol Security*) dan GRE (*Generic Routing Encapsulation*) merupakan jenis VPN yang sering digunakan untuk membentuk jaringan yang bersifat *private* dan aman.

Tujuan dari tugas akhir ini adalah bagaimana mengimplementasikan VPN berbasis IPSec dan VPN berbasis GRE, menganalisis pengaruh *sniffing, disclosure attack* dan *SYN attack* berdasarkan *vulnerabillities* jaringan terhadap layanan keamanan berupa *data confidentiality, authentication* dan *availability*. Di samping itu, akan dianalisis pengaruh dari penggunaan teknologi kriptografi tersebut terhadap parameter QoS yaitu *delay* dan *throughput*.

Kata kunci : Keamanan, VPN, IPSec, GRE , *Sniffing, Disclosure attack, SYN attack, Delay, Throughput.*