Abstrak

Instant messaging dapat diterima dan digunakan oleh organisasi untuk menjalankan aktivitas ataupun kegiatan bisnis perusahaan. Namun informasi atau pesan yang dikirimkan melalui *instant messaging* biasanya masih pesan yang berupa *plain text*. Tentunya hal ini akan menimbulkan resiko apabila pesan yang dikirimkan berupa informasi sensitif karena akan sangat mudah bagi seorang yang tidak berhak untuk menyadap informasi yang dikirimkan.

Untuk melindungi privasi pesan maka dibutuhkan mekanisme kriptografi yang menjamin bahwa pesan yang dikirimkan hanya dapat dibaca oleh orang yang tepat. Algoritma *Rijndael*(*AES*) adalah algoritma simetri yang dapat digunakan untuk proses enkripsi dan dekripsi pesan yang dikirimkan sedangkan pertukaran kunci *Diffie-Hellman* adalah metode yang dapat digunakan untuk menjamin pertukaran kunci secara aman antar dua pengguna dimana kunci ini akan digunakan pada algoritma *Rijndael*.

Dari hasil pengujian yang dilakukan pada *instant messaging* dapat diketahui bahwa penggunaan algoritma *Rijndael(AES)* dan *Diffie-Hellman Key Exchange* relatif dapat menjamin keamanan pesan yang dikirimkan dan tidak memberikan dampak waktu pengiriman pesan yang sangat signifikan bagi pengguna yang menggunakannya.

Kata kunci : pesan, enkripsi , dekripsi, pertukaran kunci, penyerang.