ABSTRAK

IMPLEMENTASI ALGORITMA RSA UNTUK PENGAMANAN PESAN PADA APLIKASI *INSTANT MESSENGER*

Oleh

Teten Nugraha
10508658

Internet hadir dengan memperkenalkan bentuk komunikasi baru dan pertumbuhannya dari tahun ke tahun sangatlah pesat. *Instant messenger* merupakan salah satu *software* yang menggunakan layanan Internet dan menjadi suatu bentuk komunikasi yang banyak digemari karena menyediakan layanan percakapan teks secara *real time*. Namun kebanyakan *instant messenger* dibangun bukan berdasarkan aspek keamanan yang harusnya menjadi bahan pertimbangan utama melainkan mengedepankan aspek-aspek bisnis. *Eavesdroppingo* atau yang lebih dikenal dengan penyadapan, menempati urutan pertama dalam kasus penyerangan dan penyadapan pesan terhadap aplikasi *instant messenger*. Oleh karena itu, diperlukan suatu sistem yang dapat mengamankan pesan sehingga privasi penggunan dapat terjaga nantinya.

Algoritma RSA yang merupakan salah satu algoritma kriptografi menawarkan mekanisme pengamanan data dengan menggunakan kunci yang berbeda, yaitu kunci publik (*public key*) untuk enkripsi pesan dan kunci privat (*private key*) untuk dekripsi pesan.

Sehingga dengan proses pengimplementasian algoritma RSA dengan aplikasi *instant messenger* diharapkan dapat menjaga keamanan pesan yang dikirim ataupun diterima oleh *client* terutama pesan yang sifatnya memerlukan tingkat privasi yang tinggi.

Kata Kunci : *Instant Messenger, Public Key, Private Key, Client*