Abstrak

Aplikasi pengiriman pesan instant (*Instant Messaging*) sudah menjadi hal yang umum digunakan oleh masyarakat luas. Kemampuan pengiriman pesan secara cepat membuat user dapat berkomunikasi satu sama lainnya secara *real-time.* Salah satu aplikasi *Instant Messaging* yang umum digunakan adalah *Yahoo! Messenger*. Aplikasi ini melakukan enkapsulasi terhadap pesan berupa plainteks (tidak menggunakan metode enkripsi), sesuai dengan protokol yang diberikan oleh *Yahoo!*. Oleh karena itu seorang *attacker* dapat membaca pesan yang dikirim dengan mudah. Agar user dapat menggunakan aplikasi *instant messaging* dengan aman, maka diimplementasikan sebuah sistem *Secure Instant Messaging.*

Aplikasi *Instant Messaging* ini dibangun menggunakan API jYMSG menggunakan bahasa pemrograman Java. Pada API jYMSG sudah disediakan protokol – protokol yang digunakan oleh *Yahoo!* sehingga pesan ter-enkapsulasi sesuai dengan protokol yang digunakan oleh *Yahoo!*.

Algoritma enkripsi yang digunakan pada sistem keamanan ini adalah *Blowfish, Twofish,* dan *AES.* hal tersebut disesuaikan dengan standar kecepatan proses dan keamanan dari ketiga metode tersebut. Pengaplikasian metode enkripsi pada aplikasi *Instant Messaging* cukup penting untuk memberikan keamanan dari serangan *attacker*. Sistem keamanan ini melakukan enkripsi terhadap pesan sebelum pesan dikirim oleh *sender* ke server *Yahoo!,* dan melakukan dekripsi saat sampai pada *receiver* sebelum pesan ditampilkan. Sehingga pesan sudah berupa cipherteks saat ditransmisikan melalui media tertentu. Pengukuran dilakukan terhadap waktu proses dan perkiraan tingkat keamanan yang diberikan oleh ketiga algoritma tersebut.

Kata kunci : *Instant Messaging, Yahoo!, jYMSG,* Algoritma enkripsi, *Blowfish, Twofish, AES,* sistem *Secure Instant Messaging.*