Abstract

Instant messaging applications has become commonly used by the public. Instant messaging capability allows the user to communicate with each other in real-time. One of the Instant Messaging application that is commonly used Yahoo! Messenger. These applications perform encapsulation of a plaintext message, according to the protocol provided by Yahoo!. Therefore, an attacker can read the messages sent with ease. So that users can use instant messaging applications with a secure, then implemented a Secure Instant Messaging system.

Instant Messaging applications are built using the API jYMSG using the Java programming language. In jYMSG API already provided protocols used by Yahoo!, so the message was encapsulated in accordance with the protocol used by Yahoo!.

Encryption algorithm used in this security system is Blowfish, Twofish, and AES. It is adjusted to the speed of the process and security standards of all three methods. Application of the method of encryption on the Instant Messaging application is important enough to provide security from attack attacker. This security system encrypts the message before the message sent by the sender to the Yahoo! servers, and perform decryption time until the receiver before the message is displayed. So the message is in the form of ciphertext when transmitted over certain media. Measurements carried out on processing time and the estimated level of security provided by the third algorithm.

Key Words : Instant Messaging, Yahoo!, jYMSG, Encryption algorithm, Blowfish, Twofish, AES, Secure Instant Messaging system.