

## ***Abstract***

*Instant messaging was accepted and used by business organization to perform their daily business activity. However the information or message that sent by instant messaging application are typically form in plain text. Therefore that will create a risk if sensitive information was sent because it can be read or sniffed by unauthorized users.*

*For protecting the confidentiality of message, it need the cryptography mechanism to guarantee the information was sent it only can be read by right person. Rijndael algorithm is symmetry algorithm it can be used for process encryption and decryption of message and Diffie-Hellman key exchange is a method for securing key exchange between two users where is the key will be used by Rijndael algorithm.*

*After the examination was performed in instant messaging, it can be known that Rindael algorithm (AES) and Diffie-Hellman Key Exchange relative can guarantee the security of the message and does not give significant time impact for process sending message to user that performed.*

***Keywords*** : *message, encryption , decryption, key exchange, attacker.*