ABSTRACT

The secure of information is being a cruacial thing in this era. Then many people try to find a way to secure the information in information exchange. One of method is with encryption method using stymmetric algorithm. However, there is a problem in using key for symmetrical algorithm, which is a key that used to encryption is same as the key for decryption, but if the key for decryption send separated that will cause the key can be detected by eavesdropper.

So to fix that problem, in this Final Project is designed an application for encryption and decryption file using Blowfish algorithm then implemented on LAN network. The key which is used to ecryption and decryption will be camouflaged and inserted along with the encrypted data, this is needed in order to avoid the key from being detected by eavesdropper. After the data that has been encrypted and sent arrive at receiver, the key that has been camouflaged and inserted will take on and used for decryption process. The testing toward the system will measure performances of Blowfish algorithm in encryption time, decryption time, time to crack the key and avalanche effect. Then the system will compared with DES algorithm, with the result is which the algorithm that most effective for implemented in file security system.

The result of implementation from this system is the data has been encrypted in network and the key which has inserted was not detected because of the key has been camouflaged. then data which arrive at receiver automatically decrypted using the key that has been inserted. Finally the system that has been designed can fix the problem in symmetric algorithm concept for sending data.

Keywords : *Cryptography, Blowfish Algorithm, Encryption, Decryption, Block Cipher.*