ABSTRACT

The development of internet in the world causes many company changes their style of bussiness through internet. For example is trading system via internet.

With the growing commerce on the Internet, many protocols protocol that is used to trade on the Internet. This protocol is used to avoid any intrusion or misuse of trade facilitation on the internet which caused the loss by either party. One of the protocols that are considered safe enough for the transaction is the i-Keyed Protocol (IKP). In this study attempted to make the emulation protocol IKP and then analyze it.

IKP (i-Keyed Protocol) is a protocol issued by IBM is intended to protect the process of trade through the Internet against the crimes - crimes that may be done via the internet. This protocol is supported by the provision of encryption facilities are quite adequate. With the use of two public key, then the buyer can only see the transactions that occur between the buyer-seller.

The purpose of this thesis is to design emulation objects used in the protocol IKP and then analyze this protocol in the application of electronic payment.

System that has been made can meet the requirement of computer network security parameter such as confidentiality, integrity, authentication, authority, and non-repudiation. System has not able to overcome man-in-the-middle attack, but it still can protect the data because it still in ciphertext form. System able to overcome brute-force attack until next few year.

Keywords: electronic payment, encryption, RSA, IKP