ABSTRACT

Authentication is the process of verifying the user's identity. Authentication is needed for computer network because the scalability of network security infrastructures is becoming a growing concern. Authentication can be classified into 2 types. There are authentication based on password and authentication based on cryptography. Authentication based on cryptography is stronger than authentication based on password. Authentication based on cryptography is suitable for use on computer network. Kerberos system is the example of authentication based on cryptography. Kerberos is the system for authentication in distributed computer system. It provides strong authentication of client and server using cryptography.

This thesis is mostly based on the Kerberos system except using asymmetric key to replace symmetric key in authentication process. The proposed technique also add hashing function technique to extend the level of security to the traditional Kerberos system. The proposed technique has 4 steps. It includes checking client, authentication request and response, ticket request and response, and application request and response. The messages that are sent via communication network will be encrypted by using asymmetric cryptography technique. Hashing function will be used to add more strength to authentication process of this proposed technique.