

Combining Diffie-Hellman Key Exchange with triple-DES to Enhance Information Security

Tin Win Maung, Thandar Thein

University of Computer studies, Yangon

constamt21@gmail.com

Abstract

Today's connected society requires secure information system to preserve data privacy and authentication un critical applications. This paper intends to implement secure information system for critical applications. The triple Data Encryption Standard (Triple-DES) algorithm has emerged to be the most commonly used in varying application because it is still reasonably secure. Diffie-Hellman key exchange (D-H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a share secret key over an insecure channel. This can then be used to encrypt subsequent communications using a symmetric key cipher. The main objective of this paper is to provide an Information Security Enhancement System by taking the advantages of Triple-DES cryptographic algorithm and D-H key exchange protocol to enhance security for information, and evaluate the Triple-DES execution times of encryption and decryption on the various data sizes.