Implementation of AES and Diffie-Hellman Algorithms in Data Sending System for Providing Security

Wint War Oo, Hnin Hnin Aye

University of Computer Studies, Yangon

wintwaroo@gmail.com, hnin2aye@gmail.com

Abstract

This paper presents our work on an implementation for data sharing system by using AES (Advanced Encryption Standard) algorithm, which is applicable in security field for providing data confidentiality. In this paper, AES is used to encrypt data with the use of a single secret key and vice versa. To improve the security of the system, secret key is exchanged using Diffie-Hellman Key Exchange Scheme dimed at creating a session key for data encryption between two parties. This system is very general and it also fulfills two requirements for secure: a strong encryption algorithm and obtaining copies of secret key in a secure fashion. We use Myanmar2 unicode version in order to enter the data into the database as Myanmar font.