Implementation of Secure Message Transmission System

Phyo Thura

University of Computer Studies, Mandalay

Phyothura2009@gmail.com

Abstract

Two secure end users want to communicate over an insecure channel. The enemy user is an outsider, listening to attack the communication. Encryption is the converting readable information as "plain text" into unreadable information as "cipher text". Advance Encryption Standard (AES) is the National Institute of Standard cipher based on the Rijndael algorithm . Digital Signature is the electronic versions of handwritten signature on electronic documents, signing using private key (only by the signer) and verification using public key(b everyone). The RSA algorithm can be used for signing and encryption. This system can perform high security message communication within web browser. This system allows encrypting Myanmar-English mixed text with a specific key, decoding encrypted messages and sending with the digital signature.