Digital Signature using RSA and MD5 Algorithms

May Thu Win, Khin Lay Myaing

University of Computer Studies, Mandalay

maythuwin456@gmail.com, myaingkhinlay@gmail.com

Abstract

Nowadays, the security of the information exchanged is very important. In this paper, MD5 is used for computing the hash value of the message and RSA is used for signing the message and verifying the digital signature. When as sender wishes to send a signed message to a receiver , the sender requests a certificate to the trusted Certification Authority. The sender hashes the plaintext and signs the hashed message with sender's private key to form a digital signature and encrypts the plaintext with receiver's public key and sends the ciphertext and signature . The receiver decrypts the ciphertext and hashes the plaintext with the same hash function from the signature. If the results are exactly equal, the signature is valid and the receiver can read the message from the sender.