Secure Telegraphy Message System Based on Hashing Algorithm MD5 and RSA Public Key Encryption

Khin Thara Phyu Nyein , Nilar Thein

University of Computer Studies, Yangon

crownnyein@gmai.com

Abstract

Telegraphy message security system relies on the privacy and authentication of information, which requires implementation of cryptographic functions, and measures are needed to protect data during their transmission. A hashing algorithm MD5 accepts an arbitrary length telegraphy message as input and produces a fixed-sized hash value or message digest. To authenticate a message, the sender computes a hash value for the message. Then, the message is encrypted to ensure that only the legal recipient can read the message contents and send the encrypted message and hash value. The receiver decrypts the incoming message. Then, it regenerates a new hash value from the decrypted message and compares the new hash value with the received hash value. If the message has been altered in transmit , there will be a mismatch.