Implementation of Secure Message Transfer System Using Controlled Trusted Center Based on RSA

Ei Chu Wai, Khaing Khaing Wai
University of Computer Studies (Yangon)
eichuwai@gmail.com, khaingkhaing.73@gmail.com

Abstract

This paper presents data transfer system between two users using the asymmetric-key cryptography. Asymmetric-key cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. A message can be encrypted with the receiver's public key and decrypted with the receiver's private key to provide security. A higher level of security can be achieved by placing controlled trusted center as a directory of public keys. Controlled Trusted Center keeps the public key of the registered users in its directoryand responsible to respond to any inquiry about the public key. The public-key announcements can include a timestamp and be signed by an authority to prevent interception and modification of the response. A signature is a technique for non-repudiation based on the public key cryptography. RSA digital signature and SHA-1 hash function are applied to provide integrity and authentication during the public key distribution. RSA encryption algorithm is also used for encryption in this secure message transfer system. RSA is two *algorithms: one for asymmetric encryption and one for signatures.*