

Secure Bank Transaction System Using Digital Signature Algorithm

Myo Min Than

University of Computer Studies, Mandalay

myominthan1@gmail.com

Abstract

In computer and network systems, the private access systems use cryptosystems that provide to certain and ensure data of information that are authentic and secure. This paper will develop the secure bank transaction system to provide authentication, non-repudiation and integrity of message using with Public key digital signature algorithm. Digital Signature Algorithm (DSA) is used for key generation, signature generation and signature verification. In signature generation, the input message is hashed with secure hash algorithm -1(SHA-1) and produces 160 bits of message digest output. The hash value and customer's private key operate in digital signature algorithm and then generates digital signature. These signature and message are sent to bank through the network. In signature verification, the received message is hashed with SHA-1. The hash value, received digital signature and customer's public key operate in DSA algorithm and produce signature, If the two signatures are the same, the signature is verified.