Secured Financial Messaging

A project by Sreeneha S

Abstract

- The aim of this project is to learn about how to establish security in financial messaging.

- The security of the system is determined by Non-Repudiation technique, which ensure data authenticity and integrity

- The important algorithms I have implemented to do so are :

  - Key generation (Private and Public keys)

  - Asymmetric Cryptography

  - Digital signatures and verification

The Flow of the problem

Key Generation for both sender and receiver.
(Public and Private)

Sender program:
- Reads the Financial message
- Encrypts the financial message
- Hashes and digitally signs the message
- Sends the encrypted message and hash to the receiver

Receiver program:
- Reads the Encrypted message
- Decrypts the financial message
- Hashes and digitally verifies the message
- Sends an acknowledgement in the same manner as above