Project Title:

Digital Signature

Submitted To:

Md. Bayazid Rahman

Lecturer

Department of CSE

NDUB

Submitted By:

Md. Harun Aur Rashid Khan Ishan

ID: 163120003

Manabendra Kishore Chakraborty

ID: 171120028

Nilima Ahmed

ID: 171120006

Batch: CSE 5

Objective: We want implement digital signature method by making a simple message sending system with java programming language & MySQL database.

Tools: Netbeans ,Xammp.

Language: Java,MySQL.

Discussion: In here we implemented digital signature method by making a simple message sending system ,where message of sender can only read by receiver of message, no other third party can avail to read the message of sender. There is also a feature where we are showing that without sender & receiver of message , nobody can avail to read the real message of them.
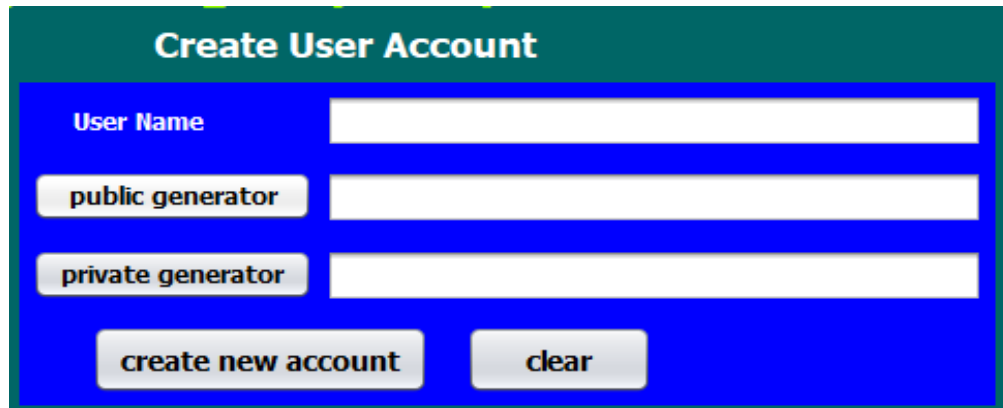
Digital Signatures with Encryption

- Alice signs the message with her private key: $S_A(M)$
- Alice encrypts the signed message with Bob's public key and sends it to Bob: $E_B(S_A(M))$
- Bob decrypts the message with his private key: $D_B(E_B(S_A(M))) = S_A(M)$
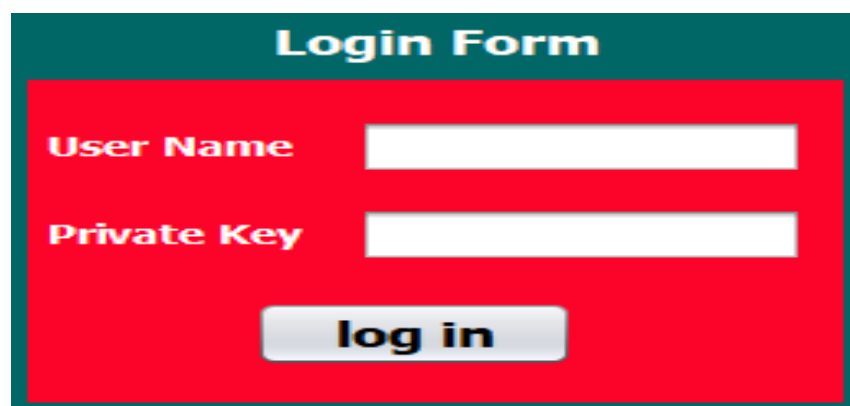- Bob verifies with Alice's public key and recovers the message: $V_A(S_A(M)) = M$
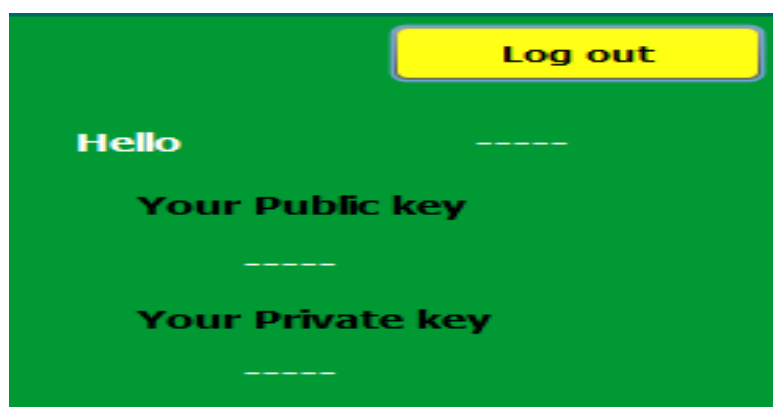
Implementation:

1. Account create.

2. Login form.

3. User information.

4. all User's details

5. Message sending feature.

6. Message inbox.

Message Inbox

Message From :   -----

Hack Test

sender public key   receiver private key

encrypted message

generate message

hack test

Conclusion: Successfully we implemented digital signature method with a simple message sending system in our computer security project using java programming language & MySQL database.