

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 ,Xampp.

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.

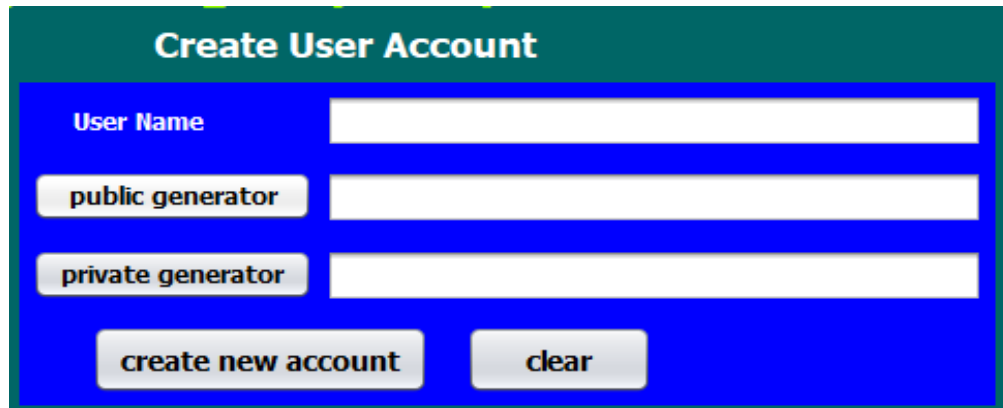


Digital Signatures with Encryption

- 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: $V_A(S_A(M)) = M$

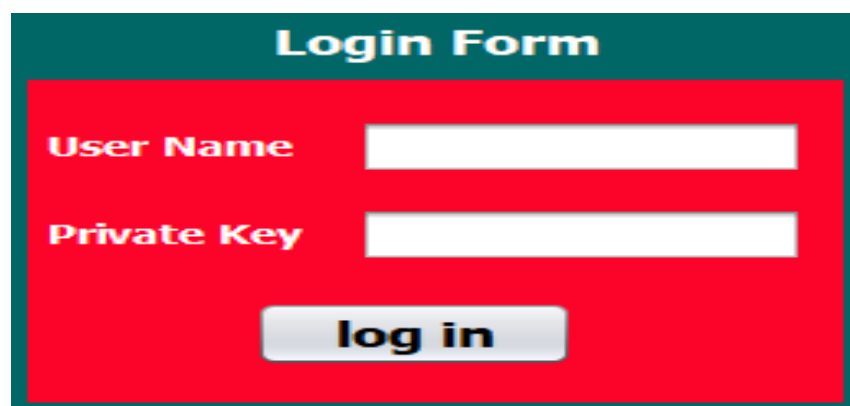
Implementation:

1. Account create.



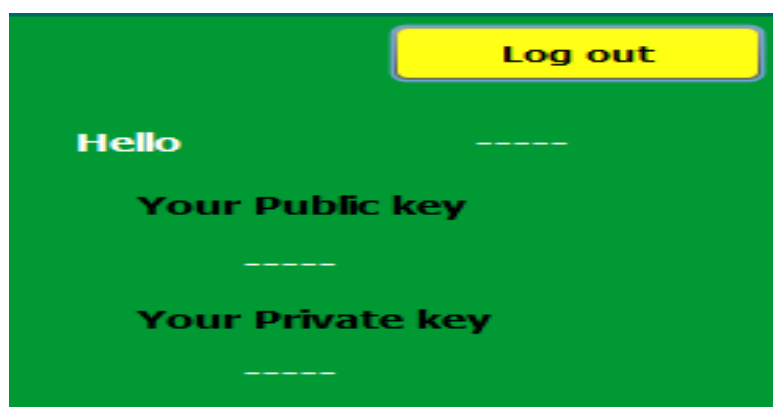
The 'Create User Account' form has a dark teal header with the title 'Create User Account' in white. The form body is blue. It contains three input fields: 'User Name', 'public generator', and 'private generator'. Each field has a corresponding label to its left. Below the input fields are two buttons: 'create new account' and 'clear'.

2. Login form.



The 'Login Form' has a dark teal header with the title 'Login Form' in white. The form body is red. It contains two input fields: 'User Name' and 'Private Key'. Each field has a corresponding label to its left. Below the input fields is a single button labeled 'log in'.

3. User information.



The 'User information' screen has a green background. At the top right is a yellow button labeled 'Log out'. Below it, the text 'Hello' is followed by a dashed line. Further down, the text 'Your Public key' is followed by a dashed line. At the bottom, the text 'Your Private key' is followed by a dashed line.

4. all User's details

All User's Details	
User Name	Public Key

5. Message sending feature.

Sent Message	
Message	<input type="text"/>
<i>to</i>	
Public Key	<input type="text"/>
Sent	
signed document	<input type="text"/>
Encryption	<input type="text"/>

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.