Cryptography and Network Security Lab-7

If Rahul wish to transfer some token to Rishabh through the Bitcoin network, then Rahul must sign a transaction with his private key so that anyone in the network can validate the transaction with Rahul's public key. In the Bitcoin network, the digital signatures are used to ensure the authentication between the Sender and receiver. Implement the digital signature generation and signature verification algorithms using the public key infrastructure like RSA to ensure the authentication, integrity, and non-repudiation services.

The steps for signature signing and verification are as follows:

Digital signing:

1. Rahul inputs a message and computes the digest of the message to be sent (Hash Value=H(M)).
2. Uses his private key (d, n) to compute the signature $S=H(M)^d \bmod n$
3. Sends the signature and message (S||M) to the receiver.

Signature verification

1. Rishabh uses Rahul's public key (e, n) to decrypt the signature and extracts the message digest $H(M)=S^e \bmod n$.
2. Subsequently, Rishabh computes the message digest H(M)' for the received message M.
3. If both message digests are identical, i.e. H(M)=H(M)', the signature is valid & integrity is ensured.

Expected Output:

<table>
<tr><th>Signature Generation (Rahul)</th><th>Signature verification (Rishabh)</th></tr>
<tr><td>Generate the private and public key</td><td rowspan="5">Receive the public key</td></tr>
<tr><td>Send public key to Rishabh</td></tr>
<tr><td>Enter the plaintext: M</td></tr>
<tr><td>Compute H(M) using SHA-160 (Library function)</td></tr>
<tr><td>Encrypt H(M) with the private key (d, n) to obtain signature: $S=H(M)^d \bmod n$</td></tr>
<tr><td>Send (S||M)</td><td>Decrypt the signature to obtain H(M) using the public key.
print: authentication is ensured</td></tr>
<tr><td></td><td>Compute H(M)' for M;
Compare: H(M)'=H(M)?
If comparison successful,
Print: message integrity is ensured.</td></tr>
</table>