# CLASS : T.E. (E&TC) SUBJECT: NETWORK SECURITY LAB

**EXPT. NO.: 09 DATE:**

Aim : Write a program to Implement Digital Signature

A Digital Signature is an authentication mechanism that enables the creator of the message to attack a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

About the experiment:

In Public key setting,it becomes difficult to verify for a receiver whether message is originated from claimed source.

In this experiment, we show how can a receiver verify integrity of the message in public key setting.

Your task is to verify, whether digital signature scheme really works and why it works?

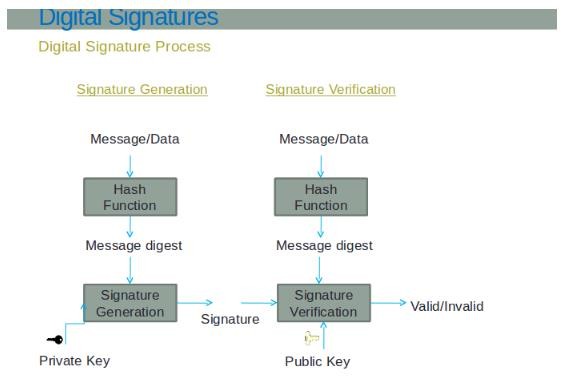
**Objective : To understand "How and Why Digital signature schemes?"**

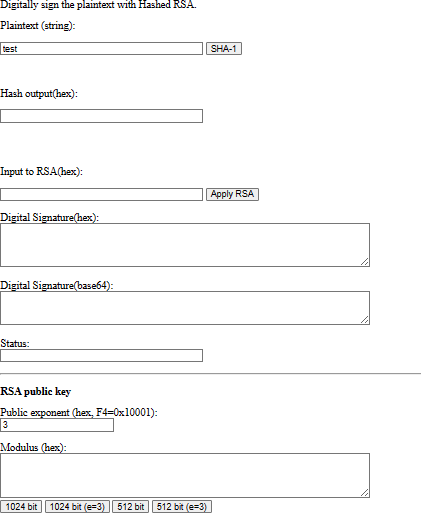
# Procedure:

# Step 1 : Enter the input text to be encrypted in the 'Plaintext' area and generate hash value for message by clicking on the SHA-1 button

Step 2 : Copy content of Hash Output(hex) field and paste it in Input to RSA(hex) field.

Step 3 : Select keysize of public key from RSA Public key section by clicking on any key button.

Step 4 : Click on Apply RSA button to generate a digital signature.



# Questions

1. Digital signature can't provide for the message

(a) Integrity

1. Congidentiality
2. NOn repudiation
3. Authentication
4. Digital signature uses for generating valid signature
   1. Private key
   2. Public key
   3. Secret key
   4. None of the above
5. Verification Algorithm uses for validating digital signature
   1. Private key
   2. Public key
   3. Secret key
   4. None of the above
6. Is digital signature scheme possible without public key cryptography

(a) Yes

1. No
2. May be exist
3. None of the above
4. Explain importance of Hashing(using experiment)and explain why Hashing is needed ?
5. Suggest a scheme that does not use any hashing scheme.
6. Explain why digital signature schemes works ?