Tutorial 6
Digital Signature

MCQ

1. ___ can be used for digital signature.

   (a) DES (b) Blowfish
   (c) RSA (d) AES

2. Which of the following is considered the strongest message digest algorithm?
   (a) SHA-1 (b) SHA-256
   (c) SHA-128 (d) SHA-512

3. To verify a digital signature, we need the ___.
   (a) Sender's private key (b) Sender's public key
   (c) Recipient's private key (d) Recipient's public key

SAQ

1. If a sender encrypts a plain text with a symmetric key and sends the cipher text to the recipient, he / she is providing _____.

2. If a sender encrypts a plain text with the recipient's public key, and sends the cipher text to the recipient, he /she is providing _____.

3. If a sender encrypts a plain text with his / her own private key, and sends the cipher text to the recipient, he / she is providing _____.

4. In digital signature, copy of signed message is identical to the original message. Suggest solutions to distinguish the copy from the original.

5. What is the important aspect that establishes trust in digital signature?

6. What is the problem with exchanging of public keys?

7. List the steps to create a digital signature.

8. List the steps to verify a digital signature.

9. With the aid of the diagram, explain how digital envelope and digital signatures can be used in together.