ASSIGNMENT : 1

UNIT : 1,2,3,4

1. Explain the following with Example
    a. Confidentiality
    b. Authentication
    c. Integrity
    d. Non Repudiation
    e. Access Control
2. Construct Playfair matrix with the Key = ENGINEERING And Encrypt the message = TEST THIS PROCESS
3. List and explain various block cipher modes of operation with the help of diagram.
4. Draw and explain the single round of DES encryption algorithm. Explain limitation of DES and also explain Avalanche effect in DES.
5. Draw AES structure with its transformation function
6. Explain RSA algorithm and list the possible approaches to attacking it.
7. Explain Diffie-Hillman Key exchange algorithm.

LAST DATE OF SUBMISSION : 25/7/2016

ASSIGNMENT : 2

UNIT : 5,6,8,9,10

1. Is message authentication code same as encryption? How message authentication can be done by message authentication code?
2. Explain different characteristics of hash function
3. Explain the ticket granting server(TGS) scheme in Kerberos.
4. Explain X.509 authentication service.
5. Which parameters define session state and which parameters define connection state in SSL(secure socket Layer)?

LAST DATE OF SUBMISSION : 16/8/2016