

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.

