PARUL INSTITUE OF ENGINEERING AND TECHNOLOGY

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

Subject Name: INS

Assignment-1

1. What is the OSI security architecture? Explain the all the types …?
2. List and briefly define the essential network and computer security requirements.?
3. List and briefly define categories of passive and active security attacks,?
4. Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.?
5. List and explain various types of attacks on encrypted message.?
6. What is the objective of attacking an encryption system? Write two approaches to attack a conventional encryption scheme.?
7. Construct a playfair matrix with key "engineering". And ecncrypt the message "test this process" .?
8. Explain one time pad scheme.?
9. Explain the various types of cryptanalytic attack, based on the amount of information known to the cryptanalyst. .?
10. Encrypt the message "Good morning" using Hill Cipher with the key
    9 4
    5 7
11. How is Steganography is different from Cryptography and write the types of Steganography.?
12. Explain Rail fence technique.?
13. What is the purpose of S-boxes in DES? Explain the avalanche effect.?
14. Draw and explain Fiestel's structure for encryption and decryption.?
15. Define confusion and diffusion and write 5 differences between them .?
16. Draw and explain Single Round of DES.?