10EC832 – Network Security

Assignment-III

Note: i) Write the assignment in a A4 size paper
iii) Mention your USN, name and section on the top right corner of first page
ii) Submit the assignment on or before 11.00 AM, Wednesday, 11/05/2016

1. With the help of a neat block diagram, explain public key cryptography.
2. Write a short note on RSA encryption algorithm.
3. Write a short note on Digital Signatures, their properties and types.
4. Explain DSS and DSA.
5. Write a short note on security of RSA.
6. Explain the various methods of distribution of public keys.
7. With suitable example, illustrate and explain Diffie-Hellman key exchange.
8. Write a short note on Elliptic Curve Cryptography.
9. Explain the need for S-Boxes in DES. Also explain how the output is generated from six input lines with the help of a neat block diagram.
10. Why S-DES was developed? Explain the structure of S-DES (Key generation and encryption of plaintext).
11. Illustrate S-DES encryption by considering Plaintext: 11111111; Key: 1111111111.

    P10: 3 5 2 7 4 10 1 9 8 6 P8: 6 3 7 4 8 5 10 9 P4: 2 4 3 1

    E/P: 4 1 2 3 2 3 4 1 IP: 2 6 3 1 4 8 5 7