USN | | | | | | | | | | 14SCS252

Second Semester M.Tech. Degree Examination, June/July 2015
Information and Network Security

Time: 3 hrs.

Max. Marks: 100

Note: *Answer any FIVE full questions.*

1   a. Explain play fair cipher with an example. Also state rules to be followed in detail. **(08 Marks)**
    b. Discuss Fiestal architecture in detail. **(08 Marks)**
    c. Describe the effects of avalanche in DES. **(04 Marks)**

2   a. Discuss the design criteria of function F. **(06 Marks)**
    b. Explain the public key encryption model with a neat diagram. **(08 Marks)**
    c. Bring out the differences between symmetric and asymmetric cryptography. **(06 Marks)**

3   a. Describe RSA algorithm with an example. **(06 Marks)**
    b. Explain Diffie – Hellman key exchange procedure. **(06 Marks)**
    c. Discuss ECC over a real number. **(08 Marks)**

4   a. Describe public –key authority method of key distribution. **(08 Marks)**
    b. What are the differences between Kerberos Version 4 and Version 5? **(08 Marks)**
    c. Write a note on federated indentify management. **(04 Marks)**

5   a. Discuss threats in wireless networks. **(10 Marks)**
    b. Explain SSL architecture with a neat diagram in detail. **(10 Marks)**

6   a. Bring out the companion of threats a web security. **(06 Marks)**
    b. Explain with a diagram how authentication and Confidentiality are implemented in PGP services. **(10 Marks)**
    c. Discuss the structure of RFC 822. **(04 Marks)**

7   a. Write the IP the architecture with diagram in detail. Also discuss IP the services. **(10 Marks)**
    b. Explain the header of the ESP with a neat diagram. Discuss the importance of padding. **(10 Marks)**

8   Write short notes on :
    a. PRNG
    b. Mutual authentication
    c. X-509 certificate
    d. IEEE802 wireless architecture. **(20 Marks)**

* * * * *