USN | | | | | | | | | | |

14SCS252

Second Semester M.Tech. Degree Examination, June/July 2016
Information and Network Security

Time: 3 hrs. Max. Marks:100

Note: ***Answer any FIVE full questions.***

1 a. Explain the Feistal Cipher structure. Also explain the various parameter and design choices which determine the actual algorithm of Feistal Cipher. **(12 Marks)**

b. Explain the Avalanche effect. **(08 Marks)**

2 a. Explain with an example the Elgamal cryptosystem. **(12 Marks)**

b. Perform encryption and decryption using the RSA algorithm for p = 3, q = 11, e = 7 and M = 5. **(08 Marks)**

3 a. Explain the following: i) Caesar cipher ii) Vernam cipher. **(10 Marks)**

b. Explain Diffie-Hellman key exchange. **(10 Marks)**

4 a. Explain with neat diagram the general format of X.509 certificate. **(08 Marks)**

b. Briefly explain four general categories of scheme for distribution of public keys. **(12 Marks)**

5 a. Differentiate between conventional encryption and public key encryption. **(05 Marks)**

b. List and briefly define types of cryptanalytic attacks based on what is known to the attacker. **(05 Marks)**

c. Explain packet exchanges and packet formation of secure shell transport layer protocol. **(10 Marks)**

6 a. Explain in detail the IEEE 802.11 WLAN. **(10 Marks)**

b. Briefly explain architecture and record protocol operations of secure sockets layer. **(10 Marks)**

7 a. What is S/MIME? Write the functions of S/MIME. **(05 Marks)**

b. Explain application of IPsec. **(05 Marks)**

c. Explain with a neat diagram encapsulating security payload format. **(10 Marks)**

8 a. Write the differences between version 4 and version 5 of Kerberos. **(10 Marks)**

b. Describe the function flow of domain keys identified mail. **(10 Marks)**

* * * * *