Total No. of Questions : 10] [Total No. of Printed Pages : 3

Roll No. .....

CS/IT–7201

B. E. (Seventh Semester) EXAMINATION, June, 2010

(Common for CS & IT Engg.)

NETWORK SECURITY

(Elective – II)

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 35

Note : Attempt any *five* questions. All questions carry equal marks.

1. (a) Explain the terms Authentication, Confidentiality, Integrity, Non-repudiation. Also give the difference between stegamography and cryptography. 10

   (b) Encrypt 'Meet me" using Hill cipher with key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Also decrypt the same. 10

Or

2. Explain S-DES. 20

3. (a) What is public key cryptography ? Explain. Bring out the difference between conventional encryption and public-key encryption. 10

   (b) Explain the schemes for distribution of public keys. 10

P. T. O.

Or

4. (a) Explain Diffie-Hellman key exchange algorithm. 10

   (b) For a Diffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$: 10

   (i) Show that 2 is a primitive root of 11.

   (ii) If user A has public key $X_A = 9$, what is A's private key X_A ?

   (iii) If user B has public key $Y_B = 3$, what is shared secret key K, shared with A ?

5. Explain SHA-1 algorithm. What basic arithmetic and logical functions are used in SHA-1 ? 20

Or

6. Why Hash functions were used to develop MAC ? Give reasons. Give design objectives of HMAC and explain the structure of HMAC. What are possible attacks ? 20

7. (a) Explain secure socket layer architecture and the SSL Record protocol. 10

   (b) Explain X·509 Authentication service in brief. 10

Or

8. (a) Give the format of Encapsulating security payload. Explain its Transport and Tunnel modes. 10

   (b) Give the differences between version 4 and version 5 of kerberos. 10

9. (a) What are the characteristics of firewall ? What are various firewall configurations ? Explain. Also give limitations of firewalls. 10

(b) Explain the following terms. Masquerador, Misfeasor, Clandestine user and Base Rate Fallacy. Explain statistical anomally detection method for intrusion detection. 10

Or

10. (a) Explain various software threats. 10

(b) Explain various types of viruses. 10