Total No. of Questions : 8] [Total No. of Printed Pages : 3

Roll No. .....

CS–7201

B. E. (Seventh Semester)
EXAMINATION, Dec., 2011
(Computer Science & Engg. Branch)
NETWORK AND WEB SECURITY
(Elective–II)
(CS–7201)

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 35

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

1. (a) With a proper diagram, bring out the taxonomy of security goals and the categorization of various security attacks while realizing these goals. 10

   (b) List the briefly define *three* classes of intruders. What are *two* common techniques used to protect a password file. 10

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

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

   (ii) If user B has public key $Y_B = 3$, what is the shared secrect key ?

P. T. O.

(b) Explain public-key cryptosystems. What are the principal elements of a public key cryptosystem ? What are the roles of the public and private keys in public key cryptosystem ? 10

3. (a) Why are message authentication codes derived from a cryptographic hash function being preferred over authentication code derived from symmetric cipher ? 10

(b) What is the function of SHA-1 ? Provide its important features. Briefly explain the outline of its compression function. 10

4. (a) What are the types of malicious software ? Briefly explain each of them. 10

(b) Describe the hierarchical organization of DNS. Also explain the fundamental properties of it. 10

5. (a) What are some weaknesses of a packet filtering router ? What is an application level gateway and circuit level gateway ? 10

(b) What comprises the basic IP sec architecture ? Describe briefly IP security documents. 10

6. (a) Using simplified DES, decrypt the string (10100010) using the key (0111111101) by hand. Show intermediate results after each (IP, F_K, SW, F_K, IP^{-1}). 10

(b) What are some threats associated with a direct digital signature scheme ? Describe in detail. 10

7. (a) Briefly describe various approaches for providing web traffic security and also compare various types of security threats on the web. 10

(b) Explain the following : 10

(i) Trusted system

(ii) Kerberos

8. Write short notes on any *four* of the following : 20

(i) Brute force attack

(ii) Hacking tools

(iii) RIPEMD

(iv) Elliptic curve cryptography

(v) SQL injection

(vi) DDOS