BE / Com / Sem VII / Rev

System Security

ws Oct Sacn- 10 49

Con. 6132–10. **(REVISED COURSE)** **GT–8835**

(3 Hours) **[Total Marks : 100**

N.B.: 1) Question No.1 is compulsory.
2) Attempt any four questions out of remaining six questions.
3) Figures to the right indicate full marks.
4) Answer to the questions should be grouped and written together.
5) Assume any suitable data wherever required but justify the same.

1. a) Explain different kinds of controls provided to secure information. 5
   b) Does VPN use Link or End to End encryption? Justify your answer. 5
   c) What are the information security goals? Explain why the balance among different goals is needed. 5
   d) What are different types of malicious code? 5

2. a) Explain Advanced Encryption Standard Algorithm in detail. 10
   b) Write a note on Kerberos system that supports authentication in distributed system. 10

3. a) Explain control of access to general objects in operating system. 10
   b) Explain nonmalicious program errors with examples. 10

4. a) In RSA system the public key of a given user is e = 7 and n = 187
      (i) What is the private key of this user? 4
      (ii) If the intercepted ciphertext is c = 11 and sent to a user whose public key is e = 7 and n = 187. What is the plaintext? 4
      (iii) What are the possible approaches to defeating the RSA algorithm? 2
   b) What is spoofing? Explain the session hijacking attack. 10

5. a) List functions of Intrusion Detection System. Explain and differentiate signature based and anomaly based IDS 10
   b) Write a detail note on Biometrics Techniques. 10

6. Write a detail note on (any two) : 20
   a) SSL Handshake Protocol
   b) Key exchange using Diffie Hellman algorithm
   c) Data Encryption Standard (symmetric key algorithm)

7. a) Explain how threat precursors are used for reconnaissance of network. 10
   b) Explain Denial of Service attacks. 10