TE/Sem VI/IT/CBGS/SWS/ 07-12-2016

System & web security

Q.P. Code : 594902

(3 Hours) **[Total Marks : 80**

N.B. : (1) Question No. **1** is **compulsory**.

(2) Attempt any **THREE** Questions out of remaining **FIVE** questions.

1. (a) Give two techniques to establish a covert channel. 5

(b) Compare and contrast discretionary access control and mandatory access control. 5

(c) Define with examples i) SQL injection ii) Cross-site scripting. 5

(d) What are the different phases of a virus? Explain. 5

2. (a) What are the different kinds of malware? How do they propagate? 10

(b) Explain RSA algorithm for public key encryption. Given modulus N = 143 and public key =7, find the values of p, q, phi (n), and private key d. Can we choose value of e=5? Justify. 10

3. (a) What is a firewall? Explain different types of firewalls and specify at which layer of the Internet stack do they operate? 10

(b) What is a denial of service attack? Discuss different ways in which an attacker can mount a DOS attack. 10

4. (a) Distinguish between the ESP and AH protocol in IPSec. Show the working of each in transport and tunnel mode. 10

(b) What is an IDS? How does it differ from a honeypot? Discuss the different types of IDS. 10

5. (a) Explain the process of generation and verification of digital certificate. 10

(b) With respect to SSL protocol explain the following:- 10

(i) Generation of master Key

(ii) Authentication of server to client.

6. Write short notes on (**any four**) : 20

(a) Windows Security

(b) Federated Identity Management

(c) Software Reverse Engineering

(d) Knapsack cryptosystem

(e) Non-malicious programming errors