Q.P. Code : **8720**

(3 Hours) [Total Marks : 100

N.B. : (1) Question **No. 1** is **compulsory**.
(2) Solve any **Four** questions from the remaining **Six** questions.
(3) Assume suitable data wherever necessary and mention the same.

1. (a) Distinguish between substitution cipher and transposition cipher. 5
(b) What are different types of malicious codes. 5
(c) What are the different types of IP - Spoofing. 5
(d) Differentiate between - vulnerability, threats and controls. 5

2. (a) A and B decide to use Diffie-Hellman key exchange where p=13, g=2. Each choose his own secret no. and exchange nos. 6 and 11. 10
(i) What is common secret key?
(ii) What are their secret nos?
(iii) Can intruder M, gain any knowledge from protocol run if he sees p, g and the 2 public keys 6 & 11. If yes, show how?
(b) Explain structure of DES. 10

3. (a) Describe block ciphers? Explain any one with example. 10

(b) Explain difference between MAC and message digest? What is role of compression function in general structure of message digest? 10

4. (a) What is Reverse Engineering? Explain need of Digital Rights Management. 10
(b) What is Buffer overflow and incomplete mediation in Software Security? 10

5. (a) How does ESP header guarantee confidentiality & integrity for packet payload? 10
(b) What makes a network vulnerable? 10

6. (a) What are different types of firewalls? Explain design, configuration and limitations. 10
(b) IPSec offers security at network layer. What is the need of SSL? Explain the services of SSL protocol? 10

7. Write Short note on **(any TWO)** 20
(a) MD5.
(b) Covert Chanel.
(c) CAPCHA.
(d) Trojan.
