TE|IT|VI (Rev.) 17/5/12
INS

53 : 1st half-12-(i)JP

Con. 3731-12. **GN–7332**

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

N.B. (1) Question No. **1** is **compulsory**.
(2) Answer any **four** out of the **remaining** questions.
(3) Answers to subsections must be answered **together**.

Q1. (a) Consider an online fees payment system. People will cast their votes through the Internet. For this system identify vulnerability, threat and attacks. (05)
(b) Define the terms Confidentiality, Integrity and Availability. Give one example each of two attacks each that violates these goals. (05)
(c) Describe any two non malicious program flaws. (05)
(d) Explain the session hijacking attack with an example. (05)

Q 2. (a) Explain clearly the differences between block and stream ciphers. (10)
(b) Give a list of network vulnerabilities with an example each. (10)

Q3.(a) Differentiate between public and private key cryptosystems. Give Examples of each type of cryptosystem. (10)
(b) Write a note on different authentication methods. (10)

Q.4. (a) Describe the various types of viruses that can infect a system. (10)
(b) What is the role of a firewall in securing a network? Describe different types of firewalls. (10)

Q.5 (a) Use two prime numbers p=3, q=5, and explain the full working of the RSA Cryptosystem. (10)
(b) Explain any two access control mechanism. Indicate clearly the advantages and disadvantages of each scheme. (10)

Q.6 (a) Explain the protocol flaws existing in the TCP/IP model that can lead to security incidents & how to overcome them. (10)
(b) What is the role of hashing? Explain any one hashing algorithm. (10)

Q.7. Write a detailed note on any one of the following topics :
(a) Intrusion Detection Systems (10)
(b) Secure Sockets Layer (SSL) (10)