

B4.5-R4: INTERNET TECHNOLOGY AND WEB SERVICES

NOTE:

1. Answer question 1 and any FOUR from questions 2 to 7.
2. Parts of the same question should be answered together and in the same sequence.

Time: 3 Hours

Total Marks: 100

1.
 - a) Write any four differences between IPv4 and IPv6.
 - b) Write short notes on Common Gateway Interface.
 - c) Briefly explain ActiveX controls.
 - d) Explain http protocol.
 - e) What is virtual reality? Write in brief on various components involved in creation of virtual reality.
 - f) Write merits and limitations of Apache and IIS Web Servers.
 - g) What is Denial of Service (DoS) attack?

(7x4)

2.
 - a) Explain in brief any six TCP/IP application protocols and write their port numbers.
 - b) Write merits and limitations (three each) of wired and wireless networks.
 - c) Write short notes on Web 2.0.

(6+6+6)

3.
 - a) What is Server-side and Client-side scripting in creation of a web application and explain the role of each?
 - b) Write six differences between java server pages (JSP) and active server pages (ASP) and explain both from the security point of view.

(9+9)

4.
 - a) Explain in detail about Simple Object Access Protocol (SOAP).
 - b) Write short notes on Web Services Description Language (WSDL).
 - c) What is Web Intelligence?

(9+6+3)

5.
 - a) What is multicast routing? Explain Distance Vector Multicast Routing Protocol with an example.
 - b) Write short notes on video streaming.
 - c) Explain in brief about H.323 protocol.

(9+6+3)

6.
 - a) Explain in detail the role of each component of LAMP (Linux, Apache, MySQL and PHP/Perl) in creation and deployment of a Web application.
 - b) How can digital certificates ensure the security of data across network?
 - c) Write short notes on open source software technologies.

(6+6+6)

7.
 - a) What is a Virtual Private Network (VPN)? Write and explain in detail about various IPSec VPN protocols.
 - b) Write in brief about security concepts such as authentication, authorization, access control, confidentiality, integrity and non-repudiation. Write names of attacks against each security parameter, in case of violation.
 - c) What are security technologies available to handle non-repudiation and message integrity?

(6+9+3)