

Tribhuvan University
Institute of Science and Technology
2074

Bachelor Level / seventh-semester / Science Full marks: 60 **Computer Science and Information Technology(CSC416)** Pass marks: 24 (Network Security) Time: 3 hours Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt any Ten questions.(6 x 10 = 60)

1. How can you differentiate data integrity from system integrity? Briefly discuss the categories of security services.
2. What is the use of master (permanent) keys in security? Write a protocol to share public keys using a public-key authority scheme.
3. What do you mean by replay attack? Discuss the roles of Authenticating Server and Ticket Granting Server in Kerberos protocol.
4. What basic security services does the SSL Record Protocol provide for SSL Connections? Mention details of the operations that the SSL Record Protocol executes for ensuring the basic security services.
5. What do you mean by local forwarding in SSH? Describe about the possible channel types recognized in SSH Connection Protocol specification.
6. How accidental and malicious associations can be threats to wireless networks. Describe the approaches to provide WAP End-to-End Security.
7. What services are defined under IEEE 802.11i RSN security specification? Discuss to IEEE 802.11i phases of operation for Authentication and Association.
8. What functionalities PGP provides for mail security? How PGP ensures confidentiality and authentication services?
9. Differentiate between Transport and Tunnel Mode. Briefly describe the fields of an Encapsulating Security Payload (ESP) packet.
10. Define cyber security and cyber war.
11. Discuss OSI security Architecture.

