Total = 5 marks.

# Answer for 2nd Class Participation Quiz.

1 marks ① Replay Attack: This is prevented by the use of nonces. client-random & server random are used as nonces. These are shared between client-server during by TLS Handshake Protocol.

1 marks ② MITM attack: This is prevented by the use of public-key certificates to authenticate the correspondents. In TLS Handshake protocol these certificates are exchanged among client and server.

1 marks ③ Password Sniffing: User data is encrypted. TLS Record Protocol provides encryption facility to ensure confidentiality. So, password sniffing is not possible under such considerations.

1 marks ④ IP Spoofing: The spoofer must be in possession of the secret key as well as the forged IP address. TLS Handshake protocol provide secure key sharing. So, confidentiality is achieved which negates the possession of secret key by attacker.

1 marks ⑤ SYN Flooding: SSL/TLS provides no protection against this attack as TLS has no control over TCP protocol in which SYN message is used.