

## COM-208: Computer Networks - Quiz 5

**Full Name:**  
**SCIPER:**

1. A public-key certificate related to Bob proves that Bob owns:
  - (a) A given public key.
  - (b) A given private key.
  - (c) A given public/private key pair.
2. To communicate securely using only symmetric key cryptography, Alice and Bob must in advance know:
  - (a) Nothing.
  - (b) A shared secret key.
  - (c) The public key of a certificate authority that both Alice and Bob trust.
3. To communicate securely using only asymmetric key cryptography, Alice and Bob must in advance know:
  - (a) Nothing.
  - (b) A shared secret key.
  - (c) The public key of a certificate authority that both Alice and Bob trust.
4. Alice wants to make a statement such that everyone in the world could verify that the statement is hers. She must use:
  - (a) A Message Authentication Code (MAC).
  - (b) A digital signature.
  - (c) Either one of them.
5. Alice sends messages to Bob over TCP (without any extra security mechanism). Persa is sitting on the channel between them. Can Persa make Bob believe that Alice sends her messages in a different order than she actually does?
  - (a) No, because TCP will put the messages back in order.
  - (b) No, because TCP will detect that the messages were reordered.
  - (c) Yes.
6. A network interface that belongs to an end-system typically has:
  - (a) No network address.
  - (b) Only a MAC address.
  - (c) A MAC address and at least one IP address.
7. What is the consequence of MAC addresses being “flat” or “non-hierarchical”?
  - (a) They all have the same length.
  - (b) They are all equally important.
  - (c) We cannot aggregate them, e.g., the way we aggregate IP addresses in IP prefixes.
8. A packet is traveling in a given IP subnet. The following must always be true:
  - (a) The packet’s source and destination MAC addresses must belong to the local IP subnet.
  - (b) The packet’s source and destination IP addresses must belong to the local IP subnet.
  - (c) The packet’s final destination must be in the local IP subnet.
9. To decide how to forward a packet, a link-layer switch:
  - (a) Looks up the packet’s destination MAC address in its forwarding table.
  - (b) Looks up the packet’s destination IP address in its forwarding table.
  - (c) Relies on the Address Resolution Protocol (ARP).
10. A link-layer switch broadcasts a packet when:
  - (a) The packet’s destination MAC address is the broadcast address.
  - (b) The switch does not have any information about the packet’s destination MAC address.
  - (c) Both of the above.