COM-208: Computer Networks - Quiz 4 (A)

Name:
SCIPER:

1. Given a network topology and link costs, will Dijstra's algorithm or Bellman-Ford produce paths with lower costs?
   (a) Dijkstra's.
   (b) Bellman-Ford.
   (c) They will produce the same paths.
2. In a link-state routing algorithm (like Dijkstra), each router computes:
   (a) a path from itself to every other router.
   (b) a path between every pair of routers in the network.
   (c) a path between every pair of end-systems in the network.
3. In a distance vector algorithm (like Bellman-Ford), each router periodically exchanges routing information with:
   (a) no other router.
   (b) all of its neighbour routers.
   (c) all the routers in the network.
4. Routers R_1, R_2, and R_3 are connected in a triangle. R_1 routes to R_3 through R_2. A poisoned reverse ensures that:
   (a) R_1 never routes to R_3 through R_2.
   (b) R_3 never routes to R_1 through R_2.
   (c) R_2 never routes to R_3 through R_1.
5. Every router on the Internet must speak at least:
   (a) one routing protocol.
   (b) one link-state routing protocol and one distance-vector routing protocol.
   (c) one intra-domain routing protocol and one inter-domain routing protocol.
6. Alice wants to send a confidential message m to Bob. Which of the following should she send?
   (a) $K_B^+\{m\}$ (m encypted with Bob's public key).
   (b) $K_A^+\{m\}$ (m encypted with her public key).
   (c) $K_A^-\{m\}$ (m encypted with her private key).
7. Alice wants to send a message m to Bob and prove that the message is from her. Appending which of the following to m would achieve this goal?
   (a) $K_B^+\{m\}$ (m encypted with Bob's public key).
   (b) $K_A^+\{m\}$ (m encypted with her public key).
   (c) $K_A^-\{m\}$ (m encypted with her private key).
8. We add nonces to message authentication codes (MACs) in order to:
   (a) prevent replay attacks.
   (b) prevent man-in-the-middle attacks.
   (c) make it harder for an attacker to break the MAC.
9. We use certificates in order to:
   (a) prevent replay attacks.
   (b) prevent man-in-the-middle attacks.
   (c) speed up encryption and decryption.
10. Alice wants to use asymmetric key cryptography to send confidential messages to many receivers. The minimum amount of information she need to have before she starts communicating with the receivers is:
    (a) a shared secret key with each receiver.
    (b) each receiver's public key.
    (c) the public key of a trusted certificate authority.

COM-208: Computer Networks - Quiz 4 (B)

Name:
SCIPER:

1. We use certificates in order to:
   (a) prevent replay attacks.
   (b) prevent man-in-the-middle attacks.
   (c) speed up encryption and decryption.
2. In a link-state routing algorithm (like Dijkstra), each router computes:
   (a) a path between every pair of routers in the network.
   (b) a path from itself to every other router.
   (c) a path between every pair of end-systems in the network.
3. Every router on the Internet must speak at least:
   (a) one routing protocol.
   (b) one link-state routing protocol and one distance-vector routing protocol.
   (c) one intra-domain routing protocol and one inter-domain routing protocol.
4. Alice wants to use asymmetric key cryptography to send confidential messages to many receivers. The minimum amount of information she need to have before she starts communicating with the receivers is:
   (a) each receiver's public key.
   (b) the public key of a trusted certificate authority.
   (c) a shared secret key with each receiver.
5. In a distance vector algorithm (like Bellman-Ford), each router periodically exchanges routing information with:
   (a) no other router.
   (b) all of its neighbour routers.
   (c) all the routers in the network.
6. Routers R_1, R_2, and R_3 are connected in a triangle. R_1 routes to R_3 through R_2. A poisoned reverse ensures that:
   (a) R_1 never routes to R_3 through R_2.
   (b) R_3 never routes to R_1 through R_2.
   (c) R_2 never routes to R_3 through R_1.
7. Alice wants to send a message m to Bob and prove that the message is from her. Appending which of the following to m would achieve this goal?
   (a) $K_B^+\{m\}$ (m encypted with Bob's public key).
   (b) $K_A^+\{m\}$ (m encypted with her public key).
   (c) $K_A^-\{m\}$ (m encypted with her private key).
8. Alice wants to send a confidential message m to Bob. Which of the following should she send?
   (a) $K_A^+\{m\}$ (m encypted with her public key).
   (b) $K_A^-\{m\}$ (m encypted with her private key).
   (c) $K_B^+\{m\}$ (m encypted with Bob's public key).
9. Given a network topology and link costs, will Dijstra's algorithm or Bellman-Ford produce paths with lower costs?
   (a) Dijkstra's.
   (b) Bellman-Ford.
   (c) They will produce the same paths.
10. We add nonces to message authentication codes (MACs) in order to:
    (a) prevent replay attacks.
    (b) prevent man-in-the-middle attacks.
    (c) make it harder for an attacker to break the MAC.