

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

Name:  
SCIPER:

- Given a network topology and link costs, will Dijkstra's algorithm or Bellman-Ford produce paths with lower costs?
  - Dijkstra's.
  - Bellman-Ford.
  - They will produce the same paths. *(Correct)*
- In a link-state routing algorithm (like Dijkstra), each router computes:
  - a path from itself to every other router. *(Correct)*
  - a path between every pair of routers in the network.
  - a path between every pair of end-systems in the network.
- In a distance vector algorithm (like Bellman-Ford), each router periodically exchanges routing information with:
  - no other router.
  - all of its neighbour routers. *(Correct)*
  - all the routers in the network.
- 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:
  - $R_1$  never routes to  $R_3$  through  $R_2$ .
  - $R_3$  never routes to  $R_1$  through  $R_2$ .
  - $R_2$  never routes to  $R_3$  through  $R_1$ . *(Correct)*
- Every router on the Internet must speak at least:
  - one routing protocol.
  - one link-state routing protocol and one distance-vector routing protocol.
  - one intra-domain routing protocol and one inter-domain routing protocol. *(Correct)*
- Alice wants to send a confidential message  $m$  to Bob. Which of the following should she send?
  - $K_B^+\{m\}$  ( $m$  encrypted with Bob's public key). *(Correct)*
  - $K_A^+\{m\}$  ( $m$  encrypted with her public key).
  - $K_A^-\{m\}$  ( $m$  encrypted with her private key).
- 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?
  - $K_B^+\{m\}$  ( $m$  encrypted with Bob's public key).
  - $K_A^+\{m\}$  ( $m$  encrypted with her public key).
  - $K_A^-\{m\}$  ( $m$  encrypted with her private key). *(Correct)*
- We add nonces to message authentication codes (MACs) in order to:
  - prevent replay attacks. *(Correct)*
  - prevent man-in-the-middle attacks.
  - make it harder for an attacker to break the MAC.
- We use certificates in order to:
  - prevent replay attacks.
  - prevent man-in-the-middle attacks. *(Correct)*
  - speed up encryption and decryption.
- 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 shared secret key with each receiver.
  - each receiver's public key.
  - the public key of a trusted certificate authority. *(Correct)*

COM-208: Computer Networks - Quiz 3 (B)

Name:  
SCIPER:

1.