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

Name:

- 1. Message Authentication Codes are used to provide
 - (a) confidentiality.
 - (b) authenticity and integrity. *(Correct)*
 - (c) resistance to man-in-the-middle attacks.
- 2. Does Dijkstra or Bellman-Ford produce better routes (if applied to the same network)?
 - (a) Dijkstra.
 - (b) Bellman-Ford.
 - (c) They produce the same routes. (Correct)
- 3. Hash(X) = first 100 bits of X
 - (a) is a bad cryptographic hash function, because it reveals information about the input. (Correct)
 - (b) is a bad cryptographic hash function, because the output is too short.
 - (c) is a good cryptographic hash function.
- 4. Asymmetric key cryptography is practical because the communicating parties
 - (a) do not need to share any data in advance.
 - (b) do not need to share any secret in advance. (Correct)
 - (c) do not need to process certificates.
- 5. A public-key certificate proves
 - (a) that a given public key belongs to a given entity. (Correct)
 - (b) that a given public key matches a given private key.
 - (c) nothing. We don't really need public-key certificates.
- 6. The forwarding process runs in
 - (a) end-hosts and determines each packet's destination IP address.
 - (b) routers and determines each packet's outgoing link. (Correct)
 - (c) routers and determines each packet's complete path.
- 7. Digital signatures differ from Message Authentication Codes in that
 - (a) they are more resistant to impersonation.
 - (b) they are more resistant to replay attacks.
 - (c) they rely on asymmetric key cryptography. (Correct)
- 8. Virtual-circuit networks are impractical because they require
 - (a) routers to handle a lot of traffic.
 - (b) routers to keep per-connection state. (Correct)
 - (c) end-hosts to keep per-connection state.
- 9. The IP prefix 1.1.1.0/16 covers IP addresses
 - (a) 1.1.1.0 to 1.1.1.255
 - (b) 1.1.1.0 to 1.1.255.255
 - (c) 1.1.0.0 to 1.1.255.255 (Correct)
- 10. If Network Address Translation (NAT) did not exist, we would need
 - (a) more network switches.
 - (b) more public IP addresses. (Correct)
 - (c) fewer public IP addresses.

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

Name:

- 1. The IP prefix 1.1.1.0/16 covers IP addresses
 - (a) 1.1.1.0 to 1.1.1.255
 - (b) 1.1.1.0 to 1.1.255.255
 - (c) 1.1.0.0 to 1.1.255.255
- 2. Digital signatures differ from Message Authentication Codes in that
 - (a) they are more resistant to impersonation.
 - (b) they are more resistant to replay attacks.
 - (c) they rely on asymmetric key cryptography.
- 3. Virtual-circuit networks are impractical because they require
 - (a) routers to handle a lot of traffic.
 - (b) routers to keep per-connection state.
 - (c) end-hosts to keep per-connection state.
- 4. Message Authentication Codes are used to provide
 - (a) confidentiality.
 - (b) authenticity and integrity.
 - (c) resistance to man-in-the-middle attacks.
- 5. The forwarding process runs in
 - (a) end-hosts and determines each packet's destination IP address.
 - (b) routers and determines each packet's outgoing link.
 - (c) routers and determines each packet's complete path.
- 6. Hash(X) = first 100 bits of X
 - (a) is a bad cryptographic hash function, because it reveals information about the input.
 - (b) is a bad cryptographic hash function, because the output is too short.
 - (c) is a good cryptographic hash function.
- 7. Asymmetric key cryptography is practical because the communicating parties
 - (a) do not need to share any data in advance.
 - (b) do not need to share any secret in advance.
 - (c) do not need to process certificates.
- 8. If Network Address Translation (NAT) did not exist, we would need
 - (a) more network switches.
 - (b) more public IP addresses.
 - (c) fewer public IP addresses.
- 9. A public-key certificate proves
 - (a) that a given public key belongs to a given entity.
 - (b) that a given public key matches a given private key.
 - (c) nothing. We don't really need public-key certificates.
- 10. Does Dijkstra or Bellman-Ford produce better routes (if applied to the same network)?
 - (a) Dijkstra.
 - (b) Bellman-Ford.
 - (c) They produce the same routes.