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

Name:

1. A router in an Autonomous System (AS) uses eBGP to distribute reachability information to
   (a) routers inside the same Autonomous System as that router.
   (b) routers inside other Autonomous Systems. *(Correct)*
   (c) neither of the above.
2. A cryptographic hash function is typically used to
   (a) provide confidentiality between the communicating parties.
   (b) encrypt public keys.
   (c) provide message authentication and message integrity. *(Correct)*
3. The network layer of the Internet offers
   (a) minimum throughput guarantees.
   (b) maximum delay guarantees.
   (c) neither of the above. *(Correct)*
4. A router running a link-state routing algorithm
   (a) needs to form a full picture of the entire network before computing the least-cost paths. *(Correct)*
   (b) uses poisoned reverse to deal with the count-to-infinity problem.
   (c) operates at the link layer (layer 2) in the protocol stack.
5. Network Address Translation (NAT) was created as a solution for
   (a) running out of available IPv4 addresses. *(Correct)*
   (b) connecting packet-switched networks with circuit-switched networks.
   (c) removing the necessity of connection tracking in routers.
6. In SSL, the client creates and sends a master key to the server which is used
   (a) to encrypt all traffic between the client and the server.
   (b) to generate 4 session keys: two for encryption and two for MAC (Message Authentication Code). *(Correct)*
   (c) by the server to verify the identity of the client.
7. A trusted Certificated Authority (CA)
   (a) digitally signs the public key of an entity to prove that the advertised public key is indeed the entity's public key. *(Correct)*
   (b) sends the public key of an entity to whomever asks for it.
   (c) provides digital signatures of private keys.
8. A nonce
   (a) is a random number that a security protocol will only use once.
   (b) is used in security protocols to protect against replay attacks.
   (c) both of the above. *(Correct)*
9. Distance-vector routing algorithms
   (a) converge slower than link-state algorithms. *(Correct)*
   (b) require more messages than link-state algorithms.
   (c) both of the above.
10. In asymmetric key cryptography, a message encrypted with the sender's private key can be decrypted with
    (a) the sender's private key.
    (b) the sender's public key. *(Correct)*
    (c) both of the above.

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

Name:

1. A cryptographic hash function is typically used to
   (a) provide confidentiality between the communicating parties.
   (b) encrypt public keys.
   (c) provide message authentication and message integrity. *(Correct)*
2. A nonce
   (a) is a random number that a security protocol will only use once.
   (b) is used in security protocols to protect against replay attacks.
   (c) both of the above. *(Correct)*
3. In SSL, the client creates and sends a master key to the server which is used
   (a) to encrypt all traffic between the client and the server.
   (b) to generate 4 session keys: two for encryption and two for MAC (Message Authentication Code). *(Correct)*
   (c) by the server to verify the identity of the client.
4. Network Address Translation (NAT) was created as a solution for
   (a) running out of available IPv4 addresses. *(Correct)*
   (b) connecting packet-switched networks with circuit-switched networks.
   (c) removing the necessity of connection tracking in routers.
5. Distance-vector routing algorithms
   (a) converge slower than link-state algorithms. *(Correct)*
   (b) require more messages than link-state algorithms.
   (c) both of the above.
6. A trusted Certificated Authority (CA)
   (a) digitally signs the public key of an entity to prove that the advertised public key is indeed the entity's public key. *(Correct)*
   (b) sends the public key of an entity to whomever asks for it.
   (c) provides digital signatures of private keys.
7. A router running a link-state routing algorithm
   (a) needs to form a full picture of the entire network before computing the least-cost paths. *(Correct)*
   (b) uses poisoned reverse to deal with the count-to-infinity problem.
   (c) operates at the link layer (layer 2) in the protocol stack.
8. The network layer of the Internet offers
   (a) minimum throughput guarantees.
   (b) maximum delay guarantees.
   (c) neither of the above. *(Correct)*
9. In asymmetric key cryptography, a message encrypted with the sender's private key can be decrypted with
   (a) the sender's private key.
   (b) the sender's public key. *(Correct)*
   (c) both of the above.
10. A router in an Autonomous System (AS) uses eBGP to distribute reachability information to
    (a) routers inside the same Autonomous System as that router.
    (b) routers inside other Autonomous Systems. *(Correct)*
    (c) neither of the above.