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

Name:

1. A man-in-the-middle attack cannot break the confidentiality of the communication between A and B when:

   (a) A and B share a secret key and use only symmetric key cryptography to encrypt their messages. *(will also be considered correct)*

   (b) A and B know each other's true public keys and use asymmetric key cryptography to encrypt their messages.

   (c) Either of the above is true (i.e., in both scenarios, confidentiality is preserved). *(Correct)*

2. An IP router has:

   (a) No MAC address.

   (b) One MAC address per network interface (per link). *(Correct)*

   (c) A single MAC address for all its network interfaces. *(will also be considered correct)*

3. The forwarding table of a link-layer switch maps:

   (a) MAC addresses to output links. *(Correct)*

   (b) IP addresses to output links.

   (c) IP addresses to MAC addresses.

4. A sends a message M to B and appends hash(key, M), where key is a shared secret between A and B. This provides:

   (a) Confidentiality.

   (b) Authenticity. *(Correct)*

   (c) Both of the above.

5. SSL prevents reordering attacks (where an adversary reorders the exchanged messages) by using:

   (a) Nonces.

   (b) Sequence numbers. *(Correct)*

   (c) Certificates.

6. Host A sends a packet to host B. The packet's destination MAC address:

   (a) Is B's MAC address.

   (b) Is the MAC address of an IP router on the path from A to B.

   (c) Can be either one, depending on the particular scenario. *(Correct)*

7. A function that outputs the first few bits of the input is a bad cryptographic hash function because:

   (a) One cannot recover the entire input from the output.

   (b) It is easy to generate multiple inputs that hash to the same output. *(Correct)*

   (c) None of the above. It is actually a good cryptographic hash function.

8. When a link-layer switch does not have an entry in its forwarding table for a packet's destination MAC address:

   (a) It drops the packet.

   (b) It forwards the packet to all the possible output links.

   (c) It forwards the packet to all the output links indicated by the spanning tree. *(Correct)*

9. Asymmetric key cryptography is more practical than symmetric key cryptography because:

   (a) It does not require sharing secrets before communication begins. *(Correct)*

   (b) It involves simpler and faster algorithms.

   (c) Both of the above.

10. The Address Resolution Protocol (ARP) maps:

    (a) MAC addresses to IP addresses.

    (b) IP addresses to MAC addresses. *(Correct)*

    (c) IP prefixes to MAC addresses.

COM-208: Computer Networks - Quiz 2 (B)

Name:

1. When a link-layer switch does not have an entry in its forwarding table for a packet's destination MAC address:

   (a) It drops the packet.
   (b) It forwards the packet to all the possible output links.
   (c) It forwards the packet to all the output links indicated by the spanning tree. *(Correct)*

2. Host A sends a packet to host B. The packet's destination MAC address:

   (a) Is B's MAC address.
   (b) Is the MAC address of an IP router on the path from A to B.
   (c) Can be either one, depending on the particular scenario. *(Correct)*

3. SSL prevents reordering attacks (where an adversary reorders the exchanged messages) by using:

   (a) Nonces.
   (b) Sequence numbers. *(Correct)*
   (c) Certificates.

4. A sends a message M to B and appends hash(key, M), where key is a shared secret between A and B. This provides:

   (a) Confidentiality.
   (b) Authenticity. *(Correct)*
   (c) Both of the above.

5. An IP router has:

   (a) No MAC address.
   (b) One MAC address per network interface (per link). *(Correct)*
   (c) A single MAC address for all its network interfaces. *(will also be considered correct)*

6. A function that outputs the first few bits of the input is a bad cryptographic hash function because:

   (a) One cannot recover the entire input from the output.
   (b) It is easy to generate multiple inputs that hash to the same output. *(Correct)*
   (c) None of the above. It is actually a good cryptographic hash function.

7. A man-in-the-middle attack cannot break the confidentiality of the communication between A and B when:

   (a) A and B share a secret key and use only symmetric key cryptography to encrypt their messages. *(will also be considered correct)*
   (b) A and B know each other's true public keys and use asymmetric key cryptography to encrypt their messages.
   (c) Either of the above is true (i.e., in both scenarios, confidentiality is preserved). *(Correct)*

8. The Address Resolution Protocol (ARP) maps:

   (a) MAC addresses to IP addresses.
   (b) IP addresses to MAC addresses. *(Correct)*
   (c) IP prefixes to MAC addresses.

9. Asymmetric key cryptography is more practical than symmetric key cryptography because:

   (a) It does not require sharing secrets before communication begins. *(Correct)*
   (b) It involves simpler and faster algorithms.
   (c) Both of the above.

10. The forwarding table of a link-layer switch maps:

    (a) MAC addresses to output links. *(Correct)*
    (b) IP addresses to output links.
    (c) IP addresses to MAC addresses.