

Question 1: Network Security is concerned with:

- A operational aspects.
- B all of the options.
- C confidentiality, integrity and authentication.
- D access and availability.

Question 2: An intruder may eavesdrop both data and control messages. However, modification, insertion and deletion of messages or their content may be even more destructive. Which layers of the networking stack can be affected by such activities?

- A The Application and Transport layers.
- B Only the Network layer.
- C Only the Application layer.
- D The Application, Transport, Network and Link layers.

Question 3: Cryptography and encryption/decryption have been widely used throughout history. However, care must be taken when handling cryptographic systems (e.g., symmetric and public key systems). Which of the following options is correct?

- A Public key systems must encrypt/decrypt **all data** using the defined public/private key pair.
- B **The method** for encoding/decoding data may be publicly known as long as secret keys (e.g., symmetric and private keys) are only known by the involved parties.
- C **The method** for encoding/decoding data **and used keys must** be kept **secret** from everyone except the sender/receiver.
- D A Certification Authority **must always** be present to **validate** the cryptographic keys.

Question 4: Using block ciphers in a simplistic way has the disadvantage that identical cleartext blocks produce identical ciphertext blocks. To solve this issue randomness can be introduced by using an Initialisation Vector (IV) in Cipher-Block Chaining (CBC). Considering this approach select the correct option:

- A CBC requires that the IV is sent securely to the receiver before initiating the communication.
- B CBC has a **negligible overhead** because after the first IV, each random block is derived from the previous block.
- C CBC has **twice the overhead** than regular cipher block encryption because it must send a new random block for each data block.
- D CBC can be used directly without need to adapt any protocols (e.g., over UDP).

Question 5: Public Key Cryptography is useful for:

- A encryption and authentication, especially for large volumes of data.
- B encryption, authentication and digital signatures.
- C encryption only.
- D digital signatures only.

Question 6: A Message Authentication Code (MAC):

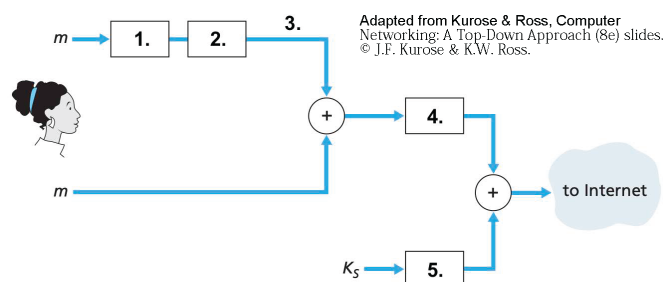
- A provides **both** message integrity and digital signatures.
- B can be used by routers to **verify** messages' integrity.
- C requires **both** a hash function and an encryption algorithm.
- D can be used by routers to uniquely identify which router created the message.

Question 7: Assume you receive an encrypted email (using your public key) allegedly signed by Alice, with an attached public key that validates the signature. Which statement is true?

- A In order to **verify** the signature you need **your own private key**.
- B You **can decrypt** the email but **not trust** that it has in fact been sent by Alice.
- C In order to **decrypt** the email you need **Alice's private key**.
- D You **can decrypt** the email **and trust** that it comes from Alice, using the attached public key without anything else.

Question 8: In this figure Alice uses symmetric key cryptography, public key cryptography, a hash function and a digital signature to provide secrecy, sender authentication and message integrity when sending an email to Bob. Considering the following nomenclature fill-in the figure's spaces from 1 to 5.

- $K_A^-(\cdot)$: Alice's Private Key
- $K_A^+(\cdot)$: Alice's Public Key
- $K_B^-(\cdot)$: Bob's Private Key
- $K_B^+(\cdot)$: Bob's Public Key
- $H(\cdot)$: Hash function
- $K_S(\cdot)$: Symmetric Key function for key K_S



- A 1. $H(\cdot)$; 2. $K_A^-(\cdot)$; 3. $K_A^-(H(m))$; 4. $K_A^+(\cdot)$; 5. $K_B^+(\cdot)$
- B 1. $H(\cdot)$; 2. $K_A^-(\cdot)$; 3. $K_A^-(H(m))$; 4. $K_S(\cdot)$; 5. $K_B^-(\cdot)$
- C 1. $H(\cdot)$; 2. $K_A^+(\cdot)$; 3. $K_A^+(H(m))$; 4. $K_S(\cdot)$; 5. $K_B^-(\cdot)$
- D 1. $H(\cdot)$; 2. $K_A^-(\cdot)$; 3. $K_A^-(H(m))$; 4. $K_S(\cdot)$; 5. $K_B^+(\cdot)$

Question 9: You receive an email that is encrypted to your public key. It also contains a digital signature and a certificate claiming to be Alice's certificate. The signature verifies using the public key in the provided certificate. Which of the following is the best answer?

- A** If a certificate is attached, it is automatically trustworthy and no further checks are needed.
- B** You still cannot be sure it was sent by Alice unless you validate that the certificate is trusted for Alice (e.g., signed by a trusted CA / valid chain to a trust anchor, correct identity binding, and not expired).
- C** If the signature verifies with the certificate's public key, then it must have been sent by Alice.
- D** Because the email is encrypted to your public key, it proves the sender is Alice.

Question 10: A routing protocol between routers uses a shared secret key and a MAC to protect routing updates. An attacker can record a valid routing update and later replay the exact same update to a router. Which of the following is the best answer?

- A** The MAC prevents replay attacks automatically, because replays will fail MAC verification.
- B** Encrypting the routing updates (confidentiality) is sufficient to prevent replay attacks.
- C** Using a longer MAC output (more bits) prevents replay attacks.
- D** A MAC alone does not prevent replay; the protocol also needs freshness information (e.g., sequence numbers, timestamps, or nonces) that the receiver checks.