RAT Test Run

Question 1: Which of the following properties applies to a hash function?

A The same input **never leads** to the **same** output.
B The output is of variable length.
C Similar messages do not lead to similar hashes.
D The same input **can lead** to **different** output.

Question 2: Which of the following attacks **cannot** be mitigated by using TLS?

A Interception of data.
B Modification of data.
C Identity theft.
D Compromise of a CA.

Question 3: Suppose a VPN is used to access "geo-blocked" content from a streaming service. At which layer is the VPN operating?

A Transport layer.
B Link layer.
C Network layer.
D Application layer.

Question 4: Suppose that an application which uses standard TCP sockets for network-based communication is used with a VPN. Which of the following statements is **false**?

A The application **does not** require TLS sockets in order to work securely.
B The application **must import IPsec** libraries in order to communicate securely.
C The application **does not need to implement IPsec** libraries in order to communicate securely.
D The application can be used **without changes**, and devices on the public Internet are **not able** to easily determine that the application uses TCP.

Question 5: Which of firewall rules are necessary to allow internal users from the 1.1.1/24 subnet to surf the Web?

	action	src addr	dst addr	proto	src port	dst port	flag
1	allow	1.1.1/24	outside of 1.1.1/24	TCP	>1023	80	ACK
2	allow	1.1.1/24	outside of 1.1.1/24	TCP	>1023	443	any
3	allow	outside of 1.1.1/24	1.1.1/24	TCP	443	>1023	ACK
4	allow	outside of 1.1.1/24	1.1.1/24	TCP	80	>1023	SYN

A 1 and 3.
B 2 and 4.
C 2 and 3.
D 1 and 4.

Question 6: Why is public key cryptography (PKC) often used together with symmetric key cryptography (SKC)?

A SKC provides integrity and authentication while PKC provides confidentiality and operational security.
B SKC allows to securely determine a shared secret while PKC is used for confidentiality.
C The exponentiation of large numbers in PKC is computationally expensive.
D Using two cryptographic schemes offers extra protection.

Question 7: Suppose Bob initiates a TLS connection to Trudy who is pretending to be Alice. During the handshake, Trudy sends Bob Alice's certificate. In what step of the TLS handshake algorithm will Bob discover that he is not communicating with Alice? Assume that Trudy **does not** have Alice's private key.

A When Trudy sends to Bob Alice's certificate because it will be invalid.
B When Bob tries to generate and encrypt the Pre-Master Secret (PMS) with the extracted public key.
C When Trudy sends Bob a HMAC of all the handshake messages.
D When Bob computes a HMAC of all the handshake messages to send to Trudy.

Question 8: Regarding the goal of message integrity, consider the following statements:

1. Message integrity is the property that the identity of the sender can be confirmed to be who or what they claim to be.
2. Message integrity is the property that the receiver can detect whether the message sent was altered in transit.
3. Both checksumming and hashing techniques may be used.
4. Generally, a hash provides a better message integrity check than a checksum.
5. To ensure message integrity, the transport layer protocol used to communication the message has to be TCP.

Select the correct option:

A Statements 2 and 5 are correct, all others are not.
B Statements 1, and 5 are correct, all others are not.
C None of the options is completely correct.
D Statements 2, 3 and 4 are correct, all others are not.

Question 9: A university launches a new web portal for students to view grades and personal information. Students must be able to access it from anywhere on the Internet (home networks, cafés, mobile data), including unmanaged devices. Which is the best security approach for protecting the data in transit?

A Require HTTPS (TLS) for the portal (e.g., redirect HTTP→HTTPS and use HSTS).

B Require a VPN and allow the portal to use HTTP inside the VPN (no TLS needed).

C Use HTTP but add a checksum to each message to prevent tampering.

D Use only password-based login; encryption in transit is not necessary if passwords are strong.

Question 10: Your team learns that a public Certificate Authority (CA) trusted by browsers has been compromised. Your organization's website uses a certificate issued by that CA. Which is the best immediate step to reduce the risk of users being tricked by a fake version of your site?

A Disable TLS temporarily until the incident is over, then re-enable it.

B No action is needed because TLS encryption still protects confidentiality even if a CA is compromised.

C Obtain and deploy a new certificate from a different (unaffected) CA and revoke/replace the old one as soon as possible.

D Switch to a self-signed certificate so attackers cannot get a "valid" certificate.