



Question 8



1 pts

The OSPF routing protocol uses a MAC (Message Authentication Code) rather than digital signatures to provide message integrity. Why do you think a MAC was chosen over digital signatures? Select one or more of the following justifications.

- ☐ MAC is easier to deploy
- ☐ Routers are generally closed systems and only the administrator can deploy keys.
- ☐ Chosen MAC over digital signatures was a legacy
- ☒ For OSPF, all routers are in a same domain, so the administrator can easily deploy the symmetric key on each router, without the need of a public key infrastructure needed for digital signatures.



Question 2

1 pts



Suppose there are two ISPs providing WiFi access in a particular café, with each ISP operating its own AP and having its own IP address block. Suppose also that by accident, each ISP has configured its AP to operate over channel 11. Will the 802.11 protocol completely break down in this situation?

☐ Yes

☒ No



Question 1



1 pts

Suppose $n = 1000$, $a = 1003$, and $b = 1009$. Use an identity of modular arithmetic to calculate $(a*b) \bmod n$. Which of the following is the correct answer?

Hint: $(a*b) \bmod n = a \bmod n * b \bmod n$. Recall: $a \bmod n$ is the remainder of a divided by n .

☒ 27

☐ 12



☐ 92

☐ 10029

Question 9

1 pts

A firewall isolates an organization's internal network from the Internet at large, allowing some packets to pass and blocking others. A firewall allows a network administrator to control access between the outside world and resources within the administered network by managing the traffic flow to and from these resources. Which of the following are true statements/ characteristics about a firewall?

-  ☒ All traffic from outside to inside and vice versa, passes through the firewall.
-  ☒ Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- ☐ It can only be implemented in Software.



Question 10

1 pts

A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large, allowing some packets to pass and blocking others. A firewall allows a network administrator to control access between the outside world and resources within the administered network by managing the traffic flow to and from these resources. Which of the following are true statements/ characteristics about a firewall?

- ☐ ☒ Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- ☐ ☐ The firewall itself is immune to penetration
- ☐ ☒ A firewall can operate as a traditional packet filter, a stateful filter, or an application gateways.
- ☒ ☒ All traffic from outside to inside and vice versa, passes through the firewall.



Question 6



1 pts

Suppose certifier.com creates a certificate for foo.com. Typically, the entire certificate would be encrypted with certifier.com's private key.

☐ True

☒ False

Question 4

1 pts

☐

Consider RSA with two prime numbers $p=7$ and $q=9$, then the value of $n =$ and the value of $z =$. Let us select $e=5$ and $d=5$, verify that these values are possible values for e and d . Using RSA public key encryption, the encoded message (Ciphertext) of $m=7$ is then equal to .

Question 3

1 pts

☐

As a mobile node gets farther and farther away from a base station, what are the two actions that a base station could take to ensure that the loss probability of a transmitted frame does not increase?

- ☐ Split-connection approaches
- ☒ Reducing the transmission rate
- ☐ TCP sender awareness of wireless links
- ☒ Increasing the transmission power

Question 5

1 pts



Select what applies to DES (Data Encryption Standard) protocol.

- ☒ It uses 56-bit symmetric key to encode a 64-bit plaintext input
- ☒ It uses 16 rounds of Mangler function application, each using a different 48-bits of the 56-bits symmetric key
- ☒ It is not secure, because it can be decrypted using a powerful hardware in less than a day

Question 7



1 pts

Confidentiality is implemented via encryption to ensure that only the sender and the intended receiver should understand message contents.

message integrity is implemented via hash function to guarantee that the sender and intended receiver exchanged messages are not altered (in transit, or afterwards) without detection. Authentication is implemented via

Digital signature so that the sender and the intended receiver confirm their identities to each other.