# Quiz 6

**Due** No due date **Points** 10 **Questions** 10 **Time Limit** 20 Minutes

**Submission Details:**

| | |
|---|---|
| **Time:** | 5 minutes |
| **Current Score:** | 7.83 out of 10 |
| **Kept Score:** | 7.83 out of 10 |

## Attempt History

| | Attempt | Time | Score |
|---|---|---|---|
| LATEST | Attempt 1 | 5 minutes | 7.83 out of 10 |

Score for this quiz: **7.83** out of 10
Submitted Jan 15 at 3:21pm
This attempt took 5 minutes.

### Question 1 — 1 / 1 pts

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

Hint: (a*b) mod n = a mod n * b mod n. Recall: a mod n is the remainder of a divided n.

- 92
- 12
- Correct! 27

a mod n = 3 , b mod n = 4. So (a*b) mod n = 3*4=12

- 10029

### Question 2 — 1 / 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
- Correct! No

### Question 3 — 1 / 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?

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

### Question 4 — 1 / 1 pts

Consider RSA with two prime numbers p=7 and q = 9, then the value of n = 63 and the value of z = 48 . 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 49 .

**Answer 1:**

Correct! 63

**Answer 2:**

Correct! 48

**Answer 3:**

Correct! 49

## Question 5 — 1 / 1 pts

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

Correct! ☑ It uses 16 rounds of Mangler function application, each using a different 48-bits of the 56-bits symmetric key

Correct! ☑ It uses 56-bit symmetric key to encode a 64-bit plaintext input

Correct! ☑ It is not secure, because it can be decrypted using a powerful hardware in less than a day

## Question 6 — 0 / 1 pts

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

Correct Answer ○ True

You Answered ◉ False

## Question 7 — 0.83 / 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.

**Answer 1:**

Correct! Confidentiality

Correct Answer Encryption

**Answer 2:**

Correct! Encryption

Correct Answer Confidentiality

Correct Answer Encryption

Correct Answer Hash Function

Correct Answer Message integrity

Correct Answer Encryption

Correct Answer Hash Function

Correct Answer Confidentiality

Correct Answer Authentication

Correct Answer Signature

Correct Answer Digital Signature

Correct Answer Authentication

**Answer 3:**

Correct! Message integrity

Correct Answer Encryption

**Answer 4:**

Correct! Hash Function

Correct Answer Confidentiality

**Answer 5:**

Correct! Authentication

Correct Answer Signature

**Answer 6:**

You Answered digital signature

Correct Answer Digital Signature

Correct Answer Authentication

## Question 8 — 1 / 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.

- ○ Chosen MAC over digital signatures was a legacy
- ○ Routers are generally closed systems and only the administrator can deploy keys.
- ○ MAC is easier to deploy
- Correct! ◉ 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 9 — 0.5 / 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?

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

## Question 10 — 0.5 / 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?

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

Quiz Score: **7.83** out of 10