Assignment 10

Due Jan 18 at 10:59am **Points** 15 **Questions** 15 **Time Limit** None

Instructions

While working on this assignment, you certify that you have neither given help to nor received help from any other person.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	77 minutes	12 out of 15

Submission Details:

Time:	77 minutes
Current Score:	12 out of 15
Kept Score:	12 out of 15

ⓘ Correct answers are hidden.

Score for this quiz: **12** out of 15
Submitted Jan 15 at 5:15pm
This attempt took 77 minutes.

Question 1 1 / 1 pts

In the Diffie-Hellman (DH) public-key encryption algorithm, which allows two entities to agree on a shared key. The DH algorithm makes use of a large prime number p and another large number g less than p. Both p and g are made public (so that an attacker would know them). In DH, Alice and Bob each independently choose secret keys, SA and SB, respectively. Alice then computes her public key, TA, by raising g to SA and then taking mod p. Bob similarly computes his own public key TB by raising g to SB and then taking mod p. Alice and Bob then exchange their public keys over the Internet. Alice then calculates the shared secret key S by raising TB to SA and then taking mod p. Similarly, Bob calculates the shared key S′ by raising TA to SB and then taking mod p. Will Alice and Bob obtain the same symmetric key, that is, S=S′?

- ○ No
- ◉ Yes

Partial

Question 2 0.5 / 1 pts

https (secure http) is generally used and is now replacing http.

- ☑ This is true because https uses ssl over TCP, and implements symmetric key and public key algorithms]
- ☐ All https protocols use one complex symmetric key that is hard to break
- ☐ This is true and is becoming a default for all websites and it is impossible to intercept https communication
- ☐ This is true only in online shopping and banking websites

Question 3 1 / 1 pts

[True or False] Consider RSA with p=3 and q=11, then possible values of e and d are 9 and 9.

- ◉ True
- ○ False

Question 4 1 / 1 pts

[True or False] IDS: intrusion detection system provides packet filtering that operates on TCP/IP headers only and examines correlation among multiple packets through port scanning, network mapping and DoS attacks.

- ◉ True
- ○ False

Question 5 1 / 1 pts

Firewalls are generally used to:

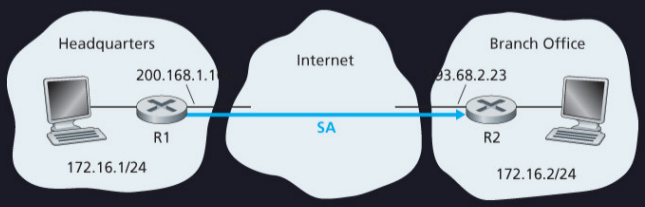
- [x] allow only authorized access to inside network
- [x] prevent denial of service attacks
- [x] prevent illegal modification/access of internal data

Partial

Question 6

0.5 / 1 pts

Consider the following diagram and suppose Trudy is a woman-in-the-middle, who can insert datagrams into the stream of datagrams going from R1 and R2. As part of a replay attack, Trudy sends a duplicate copy of one of the datagrams sent from R1 to R2. Will R2 decrypt the duplicate datagram and forward it into the branch-office network?



- [x] If Trudy does not bother to change the sequence number, R2 will detect the duplicate when checking the sequence number in the ESP header.
- [ ] If Trudy increments the sequence number, the packet will fail the integrity check at R2.

Question 7

1 / 1 pts

[True of False] The operations through which Alice can communicate with PGP to provide confidentiality, authentication, and integrity include: symmetric key cyptography, public key cryptography, a hash function, and a digital signature to provide secrecy, sender authentication, and message integrity.

- (•) True
- ( ) False

Question 8

1 / 1 pts

Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K+B,K−B), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(·). Is it possible to design a scheme so that Bob can verify that Alice created the message?

- ( ) Yes, with Bob's certificate
- (•) No, without a public-private key pair or a pre-shared secret, Bob cannot verify that Alice created the message.,

Question 9

1 / 1 pts

Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K+B,K−B), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(·). Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob?

- ( ) No, Alice needs public - private key pairs
- (•) Yes, Alice simply encrypts the message with Bob's public key and sends the encrypted message to Bob.

Question 10

1 / 1 pts

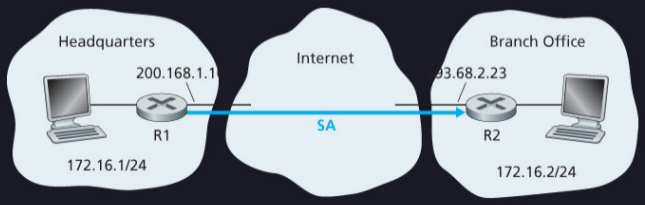
[True of False] Consider sending a TCP segment from a host in 172.16.1/24 to a host in 172.16.2/24. Suppose the acknowledgment for this segment gets lost, so that TCP resends the segment. Because IPsec uses sequence numbers, R1 will not resend the TCP segment.

- ( ) True
- (•) False

Question 11

1 / 1 pts

[True or False] Consider the following diagram:



When a host in 172.16.1/24 sends a datagram to an Amazon.com server, the router R1 will encrypt the datagram using IPsec.

- True
- False

Incorrect

Question 12

0 / 1 pts

In 4G LTE cellular systems, what is an International Mobile Subscriber Identity (IMSI)?

- Assigned by a mobile carrier network to a device, when the device attaches to the radio access network, serving a similar link-layer role as MAC addresses in a wired network.
- A 64-bit identifier that identifies the cellular network to which an mobile subscriber is attaching. Somewhat analogous to the Autonomous System (AS) number used in BGP to identify/name networks.
- A 64-bit identifier stored on a cellular SIM (Subscriber Identity Module) card that identifies the subscriber in the worldwide cellular carrier network system.
- A fancy name for a globally unique phone number, including country code.

Not quite. This answer is incorrect.

Question 13

1 / 1 pts

Which of the following statements is true about the link-level service of reliable data transfer (using ACKs) in WiFi (802.11) networks and in 4G cellular networks?

- LTE provides link-level reliable data transfer but WiFi does not.
- WiFi provides link-level reliable data transfer but LTE does not.
- Both WiFi and LTE provide link-level reliable data transfer.

Nice! This answer is correct.

- Neither WiFi nor LTE provide link-level reliable data transfer.

Nice! This answer is correct.

Incorrect

Question 14

0 / 1 pts

Which of the following statements is true about "sleep modes" that allow a wireless device to "sleep" and occasionally "wake up" as a technique for saving battery life?

- Both WiFi and LTE provide sleep modes.
- WiFi provides sleep modes but LTE does not.
- Neither WiFi nor LTE provide sleep modes.
- LTE provides sleep modes but WiFi does not.

Not quite. This answer is incorrect.

Question 15

1 / 1 pts

Which of the following statements is true about how 4G cellular networks (operated by different carriers/ companies) connect together?

- In a 4G network, the radio access network connects to the legacy phone network for voice calls, but to the public Internet for data connections.
- 4G networks connect to each other using the existing phone interconnection networks from earlier 3G and 2G networks.
- 4G networks are generally all-IP, and so cellular networks interconnect (peer) directly to each other, or peer at the cellular equivalents of the Internet Exchange Points that we saw used for interconnecting wired networks in the public Internet.

Nice! This answer is correct.

Nice! This answer is correct.

Quiz Score: **12** out of 15