**Tutorial / Practice #8**

**Cloud Security INTE2401/2402**

**1. Multiple Choice Question**

(1) In SSL handshake protocol, server authentication is \_\_\_ and client authentication is \_\_\_\_.

A. Mandatory; Mandatory

B. Mandatory; Optional

C. Optional; Mandatory

D. Optional; Optional

(2). In SSL, a protocol for transferring data using a variety of predefined cipher and authentication combinations is called

A. Handshake protocol

B. Authentication protocol

C. Record protocol

D. Cipher protocol

(3) In SSL record protocol, the message is

A. Compressed at first and then encrypted.

B. Encrypted at first and then compressed.

C. Encrypted without compression.

D. Compressed without encryption.

(4) In SSL, Alert Protocol may be invoked by \_\_\_\_.

A. close\_notify

B. Handshake protocol error

C. Record protocol error

D. All the above

(5) In SSL, Ephemeral Public Keys are used for

A. Forward security

B. Semantic security

C. Security against the man-in-the-middle attack

D. Security against the chosen ciphertext attack

(6) Diffie-Hellman key agreement protocol is insecure because it is vulnerable to \_\_\_.

A. Known plaintext attack

B. Dictionary attack

C. Eavesdropping attack

D. Man-in-the-middle attack

(7) IPSec Architecture includes \_\_\_\_\_\_\_\_\_ .

A. Authentication Header (AH)

B. Encapsulating Security Payload (ESP)

C. Internet Key Exchange (IKE)

D. All the above

(8) IPSec provides security to \_\_\_\_\_\_ communications.

A. Host-to-Host

B. Host-to-Gateway

C. Gateway-to-Gateway

D. All the above

(9) IPSec operates in \_\_\_\_\_\_ .

A. Transport mode

B. Tunnel mode

C. Either A or B

D. Neither A nor B

(10) Virtual Private Networks (VPN) can be created by

A. Transport mode

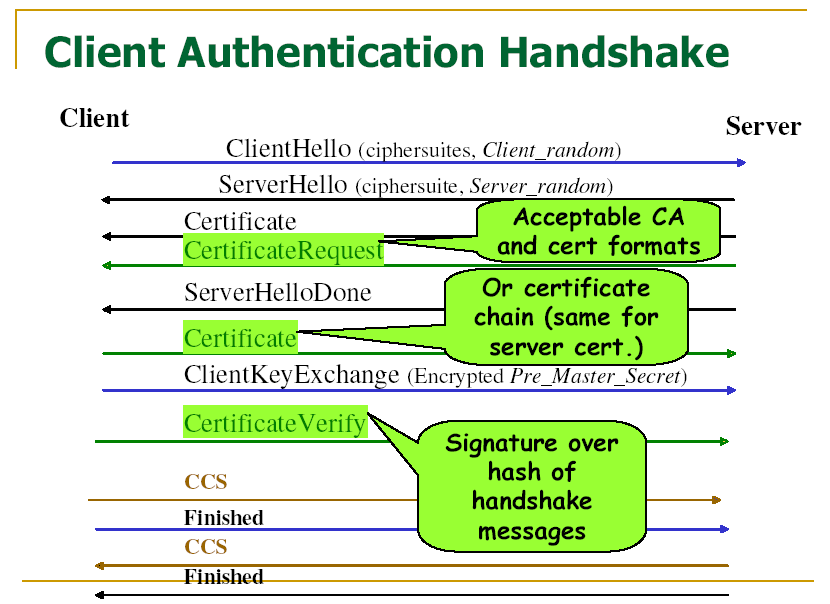
B. Tunnel mode

C. Both A and B

D. Neither A nor B

**2. Conceptual and Computational Questions**

(1) For SSL handshake protocol, server authentication is mandatory and client authentication is optional. Describe SSL handshake protocol with both client and server authentication.



(2) Suppose that Alice and Bob wish to secure their communication over the public network, e.g., the Internet. They do not have prior knowledge, such as a secret key shared in advance. Therefore, Alice and Bob decide to use the Diffie-Hellman key exchange protocol to establish a secret key. Alice chooses a prime number p=12203 and g=179 (a primitive root of p) as the public parameters. Then she chooses a=1234 and sends (p, g, ga(mod p)) to Bob. Bob chooses b=5678 and send gb(mod p) back to Alice.

a. What is the secret key they share after the Diffie-Hellman key change?

b. Perform a man-in-the-middle attack to the Diffie-Hellman key exchange protocol. Show steps.

**3.Programming Questions**

1. Implement 160-bit random number generation.

Potential solution: [here](http://titan.csit.rmit.edu.au/~e23700/2022/cloud/lab8/1/)

1. Implement RSA encryption and decryption algorithms.

Potential solution: [here](http://titan.csit.rmit.edu.au/~e23700/2022/cloud/lab8/2)

1. Apply AWS educate account via https://aws.amazon.com/education/awseducate/ or create AWS personal account via https://aws.amazon.com.