Question 3

Not yet answered

Marked out of 2

Flag question

Modification of message and Denial of Service (DoS) are passive attacks

Select one:

- True
- False

Question 4

Not yet answered

Marked out of 2

Flag question

TLS **abbreviated** handshake have Which of the following

- a. Session resumed from an old state
- b. All of them
- c. key material exchanged
- d. Authentication

Clear my choice

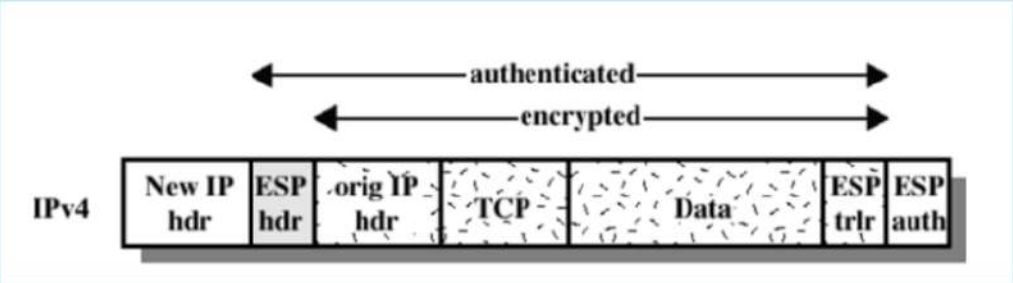
Question 5

Not yet answered

Marked out of 2

Flag question

Which of the following mode used in the diagram?



- a. AH Transport Mode
- b. ESP Tunnel Mode
- c. AH Tunnel Mode
- d. ESP Transport Mode

Clear my choice

Question 6

Not yet answered

Marked out of 2

Flag question

Match the following security protocols with their corresponding network layers?

Wi-Fi Security	Data Link Layer
IPsec	Network Layer
S/MIME, PGP – email security	Application Layer
SSL / TLS	Transport layer

Question 7

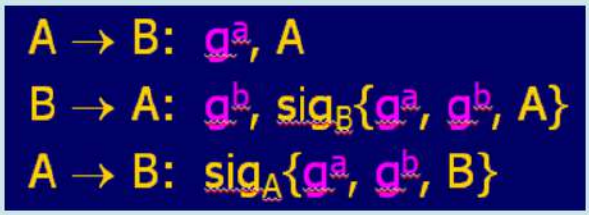
Answer saved

Marked out of 1

Flag question

The following is correct steps for

•Shared secret:
•Authentication
•Identity protection



Select one:

- ○ True
- ◉ False

Question 8

Answer saved

Marked out of 2

Flag question

Which of the following protocol client and server use public-key cryptography to establish a shared secret key between the client and the server

- ○ a. Record protocol
- ◉ b. Handshake protocol

Question 9

Not yet answered

Marked out of 2

Flag question

Match the following IP sec Mode with their corresponding functions?

IP header is not protected (except some fields) — Transport Mode

Actually puts all IP packet within another (outer) one — Tunnel Mode

Question 10

Not yet answered

Marked out of 2

Flag question

Transport Layer Security protocol, version 1.0 based on which of the following protocol

- a. SMIME
- b. IP Security
- c. SSL ver 3.0
- d. None of them

Clear my choice

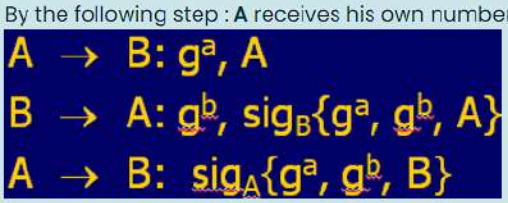
Question 11

Answer saved

Marked out of 2

Flag question

By the following step : **A** receives his own number m signed by B's private key and deduces that B is on the other end;



Select one:

- True
- False

Question 12

Not yet answered

Marked out of 2

Flag question

In which of the following the malicious participant should not be able to exploit the protocol to cause the other party to waste resources

- a. Shared secret
- b. Authentication
- c. Identity protection
- d. Protection against denial of service

Question 16

Not yet answered

Marked out of 1

Flag question

There is no actual cryptography in intruder model

Select one:

- (●) True
- ( ) False

Question 17

Not yet answered

Marked out of 2

Flag question

Match the following security cryptographic items with their corresponding functions?

RSA, DSS, SHA-1	Number theory
SSL, IPSec, ..	Protocols and policies
Firewalls, intrusion	Implementation

Question 18

Not yet answered

Marked out of 1

Flag question

Modeling JFK in applied pi calculus

Select one:

- (●) True
- ( ) False

Question 19

Not yet answered

Marked out of 2

Flag question

Which of the following attacker can flood a server with requests, overloading the server resources

- ( ) a. Eavesdropping
- (●) b. Denial of Service
- ( ) c. Man-in-the-Middle
- ( ) d. Client Imposter & Server Imposter

Clear my choice

Question 20

Not yet answered

Marked out of 1

Flag question

After the TLS protocol has finished, client and server should agree on their shared secret

Select one:

- True
- False

Question 1

Not yet answered

Marked out of 2

Flag question

"Rational derivation" of the JFK protocol provides which of the following

- a. All the above
- b. shared secret creation
- c. Authentication
- d. Identity protection
- e. DoS protection

Clear my choice

Question 2

Not yet answered

Marked out of 2

Remove flag

Which of the following is correct for IP Security protocol

- a. IPSec = AH + ESP + SA
- b. IPSec = AH + ESP + IPcomp
- c. IPSec = AH + ESP