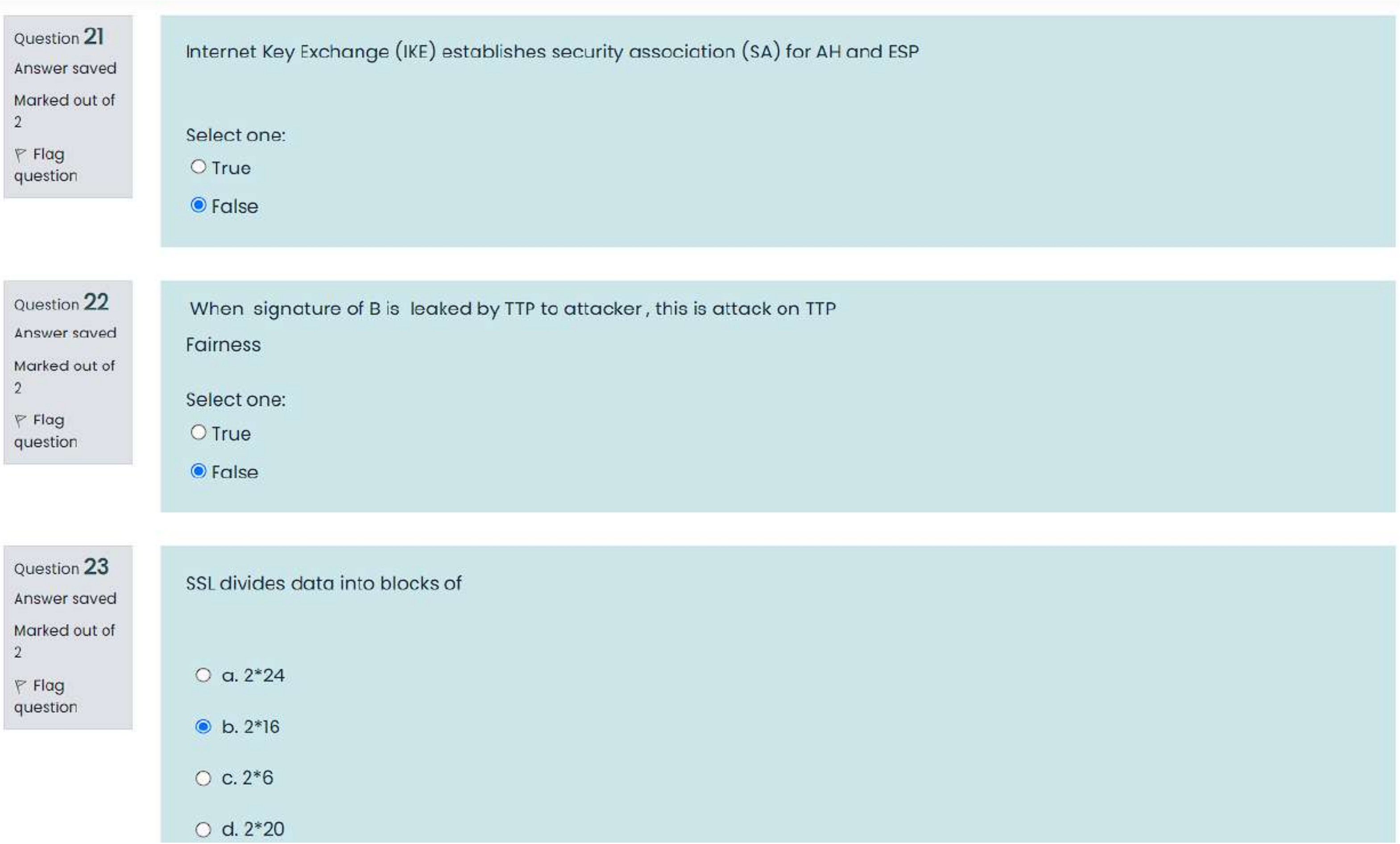


Question 21

Answer saved

Marked out of 2

Flag question

Internet Key Exchange (IKE) establishes security association (SA) for AH and ESP

Select one:

○ True

● False

Question 22

Answer saved

Marked out of 2

Flag question

When signature of B is leaked by TTP to attacker , this is attack on TTP

Fairness

Select one:

○ True

● False

Question 23

Answer saved

Marked out of 2

Flag question

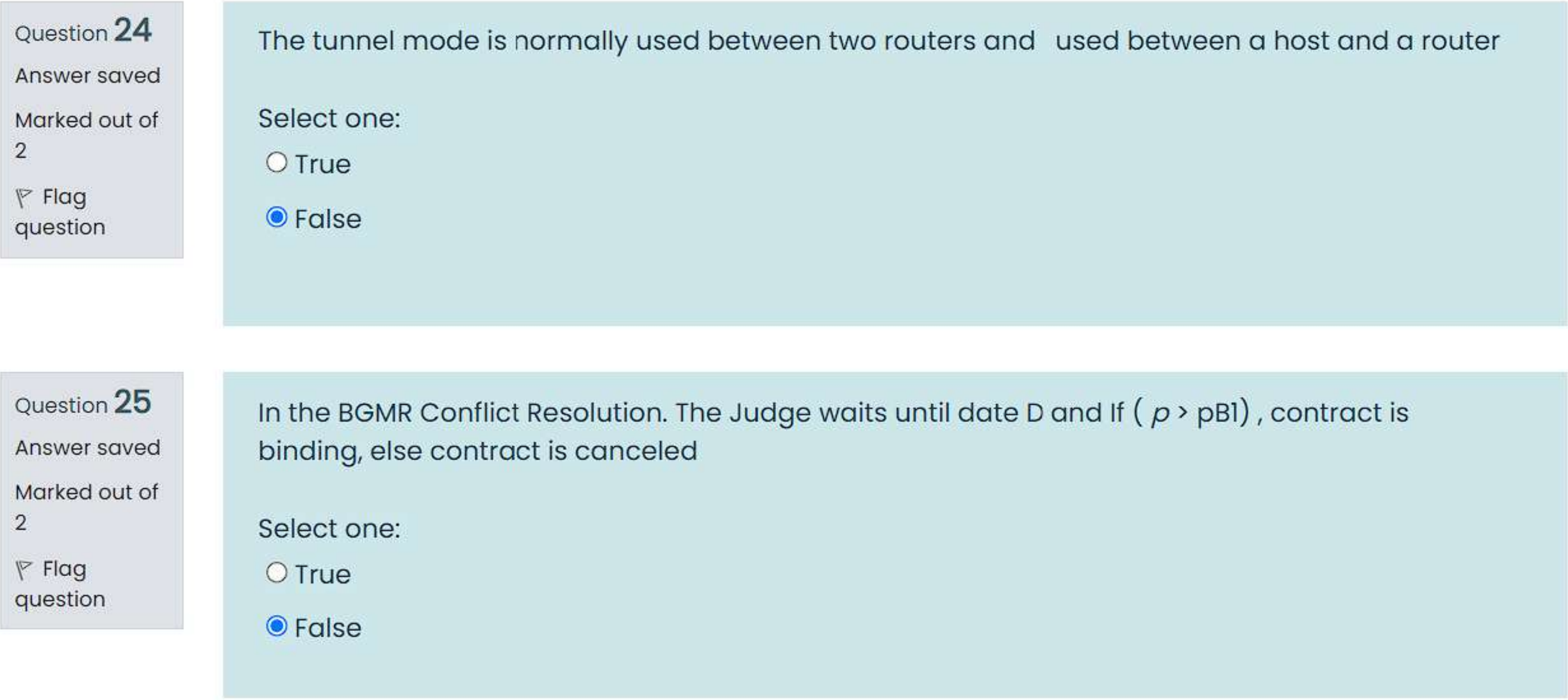
SSL divides data into blocks of

○ a. 2*24

● b. 2*16

○ c. 2*6

○ d. 2*20



Question 24

Answer saved

Marked out of 2

Flag question

The tunnel mode is normally used between two routers and used between a host and a router

Select one:

○ True

● False

Question 25

Answer saved

Marked out of 2

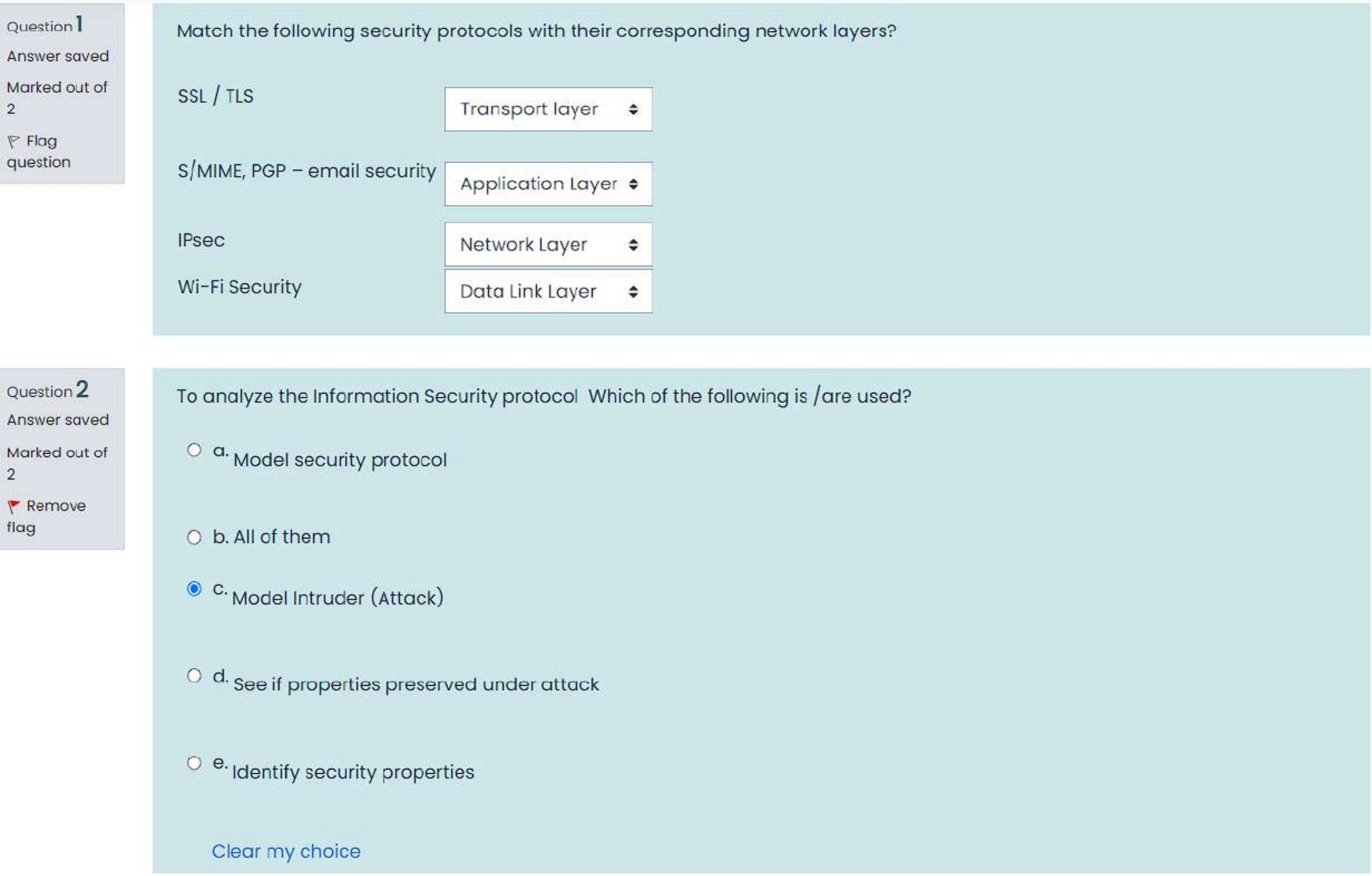
Flag question

In the BGMR Conflict Resolution. The Judge waits until date D and If (p > pB1) , contract is binding, else contract is canceled

Select one:

○ True

● False



Question 1

Answer saved

Marked out of 2

Flag question

Match the following security protocols with their corresponding network layers?

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

Question 2

Answer saved

Marked out of 2

Remove flag

To analyze the Information Security protocol Which of the following is /are used?

○ a. Model security protocol

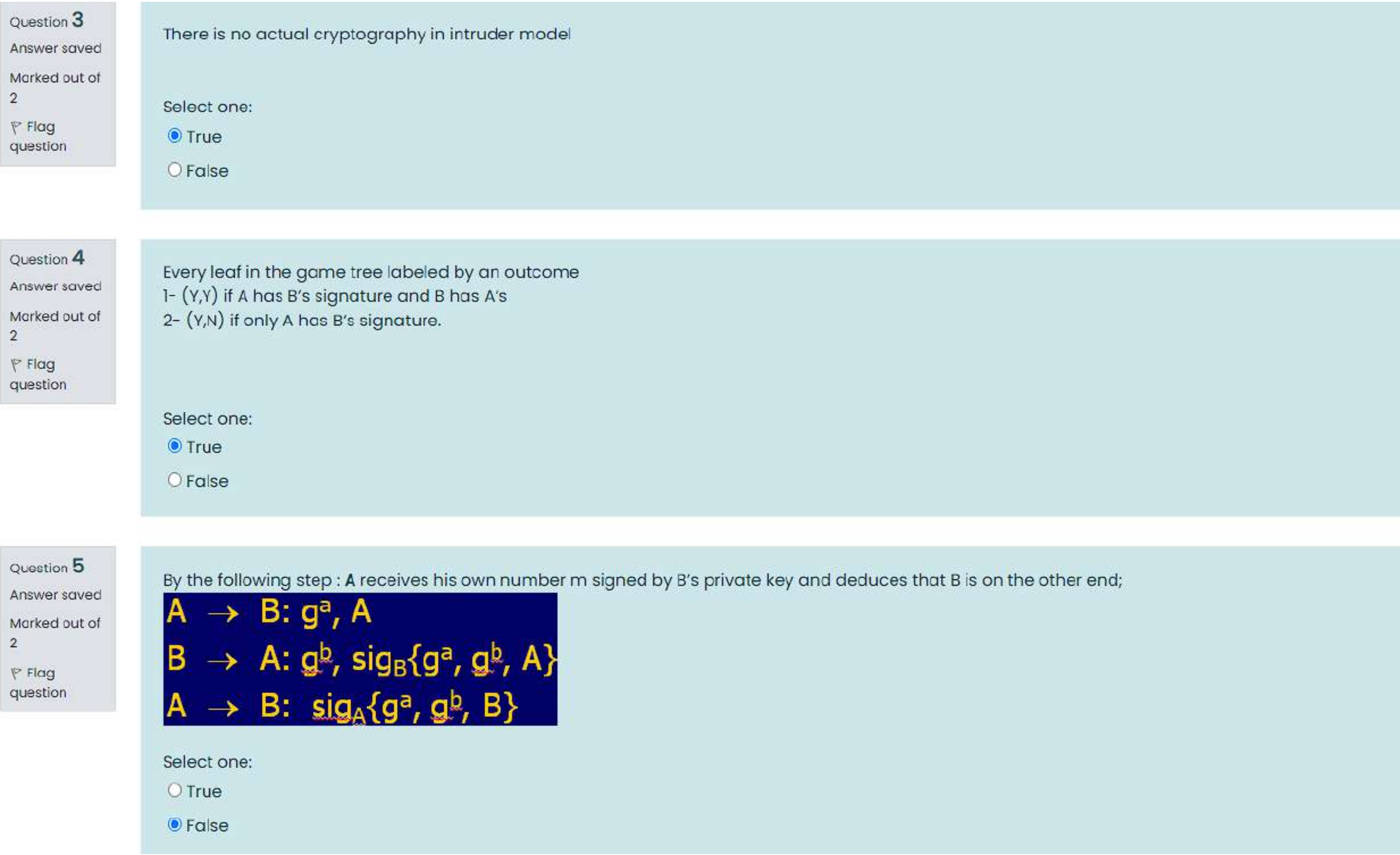
○ b. All of them

● c. Model Intruder (Attack)

○ d. See if properties preserved under attack

○ e. Identify security properties

Clear my choice



Question 3
Answer saved
Marked out of 2
Flag question

There is no actual cryptography in intruder model

Select one:

● True

○ False

Question 4
Answer saved
Marked out of 2
Flag question

Every leaf in the game tree labeled by an outcome
1- (Y,Y) if A has B's signature and B has A's
2- (Y,N) if only A has B's signature.

Select one:

● True

○ False

Question 5
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;

$A \rightarrow B: g^a, A$

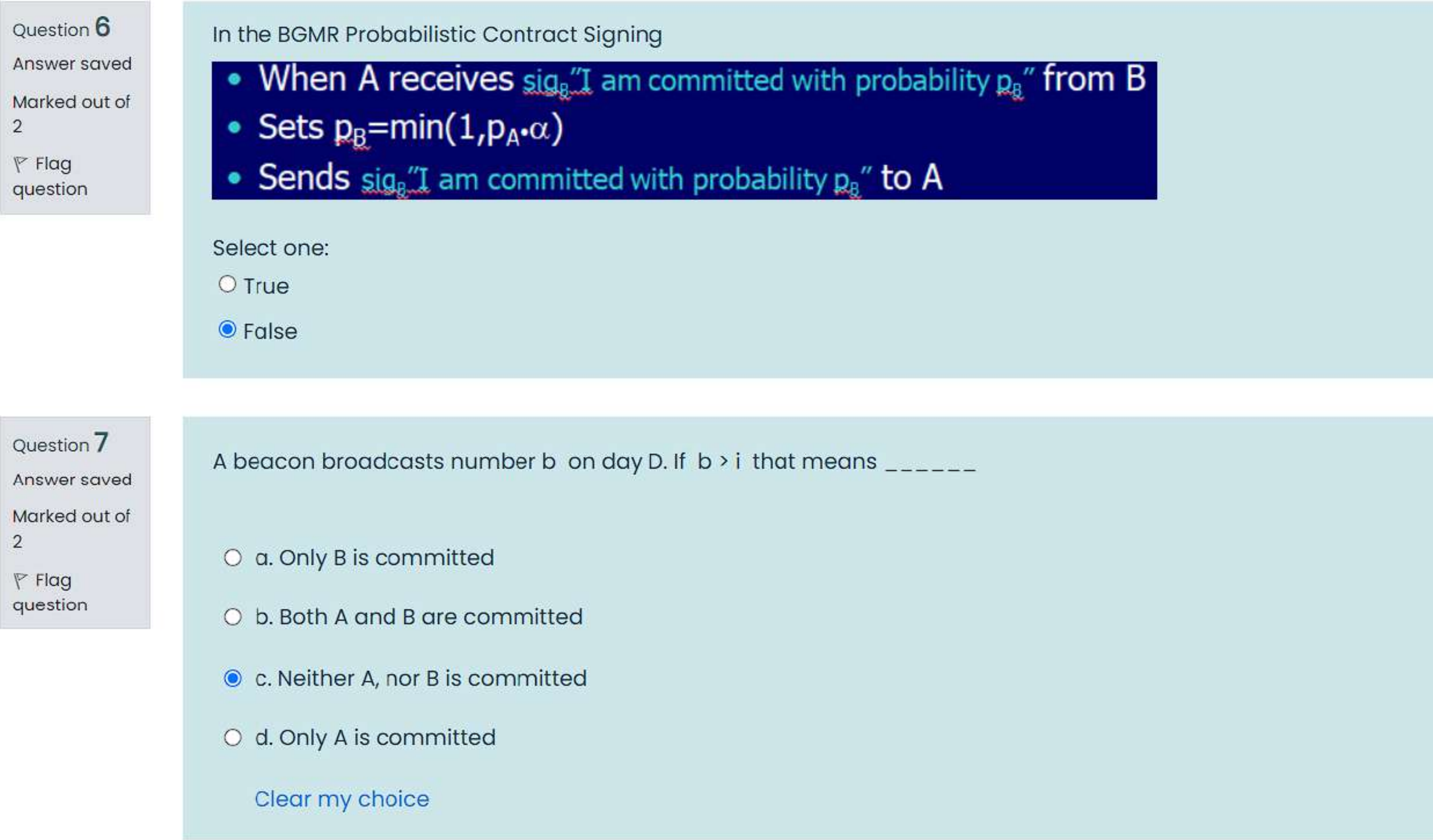
$B \rightarrow A: g^b, sig_B\{g^a, g^b, A\}$

$A \rightarrow B: sig_A\{g^a, g^b, B\}$

Select one:

○ True

● False



Question 6

Answer saved

Marked out of 2

Flag question

In the BGMR Probabilistic Contract Signing

- When A receives sig_B"I am committed with probability p_B" from B
- Sets $p_B=\min(1,p_A\cdot\alpha)$
- Sends sig_B"I am committed with probability p_B" to A

Select one:

○ True

● False

Question 7

Answer saved

Marked out of 2

Flag question

A beacon broadcasts number b on day D. If b > i that means ______

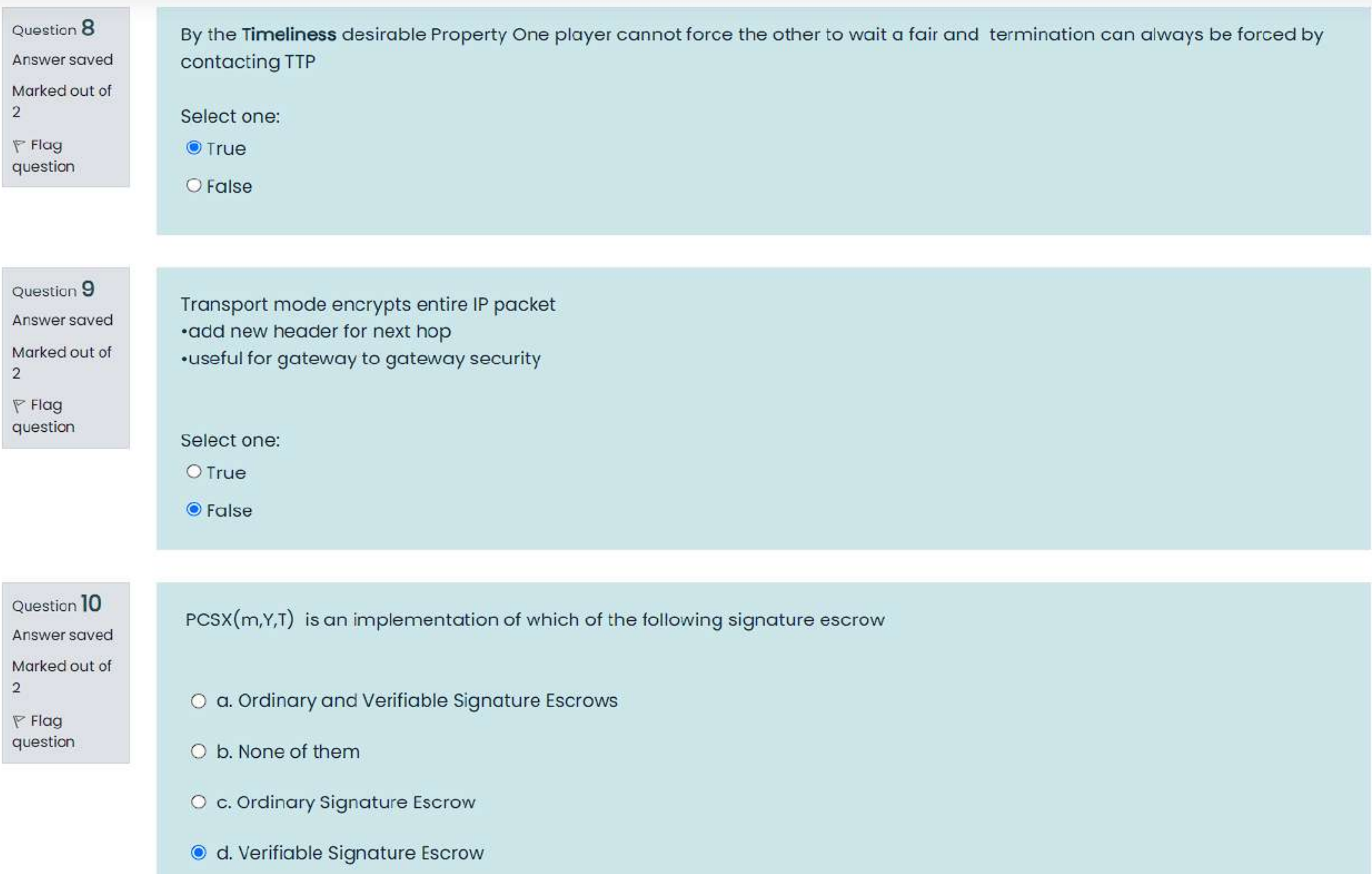
○ a. Only B is committed

○ b. Both A and B are committed

● c. Neither A, nor B is committed

○ d. Only A is committed

Clear my choice



Question 8

Answer saved

Marked out of 2

Flag question

By the **Timeliness** desirable Property One player cannot force the other to wait a fair and termination can always be forced by contacting TTP

Select one:

● True

○ False

Question 9

Answer saved

Marked out of 2

Flag question

Transport mode encrypts entire IP packet

•add new header for next hop

•useful for gateway to gateway security

Select one:

○ True

● False

Question 10

Answer saved

Marked out of 2

Flag question

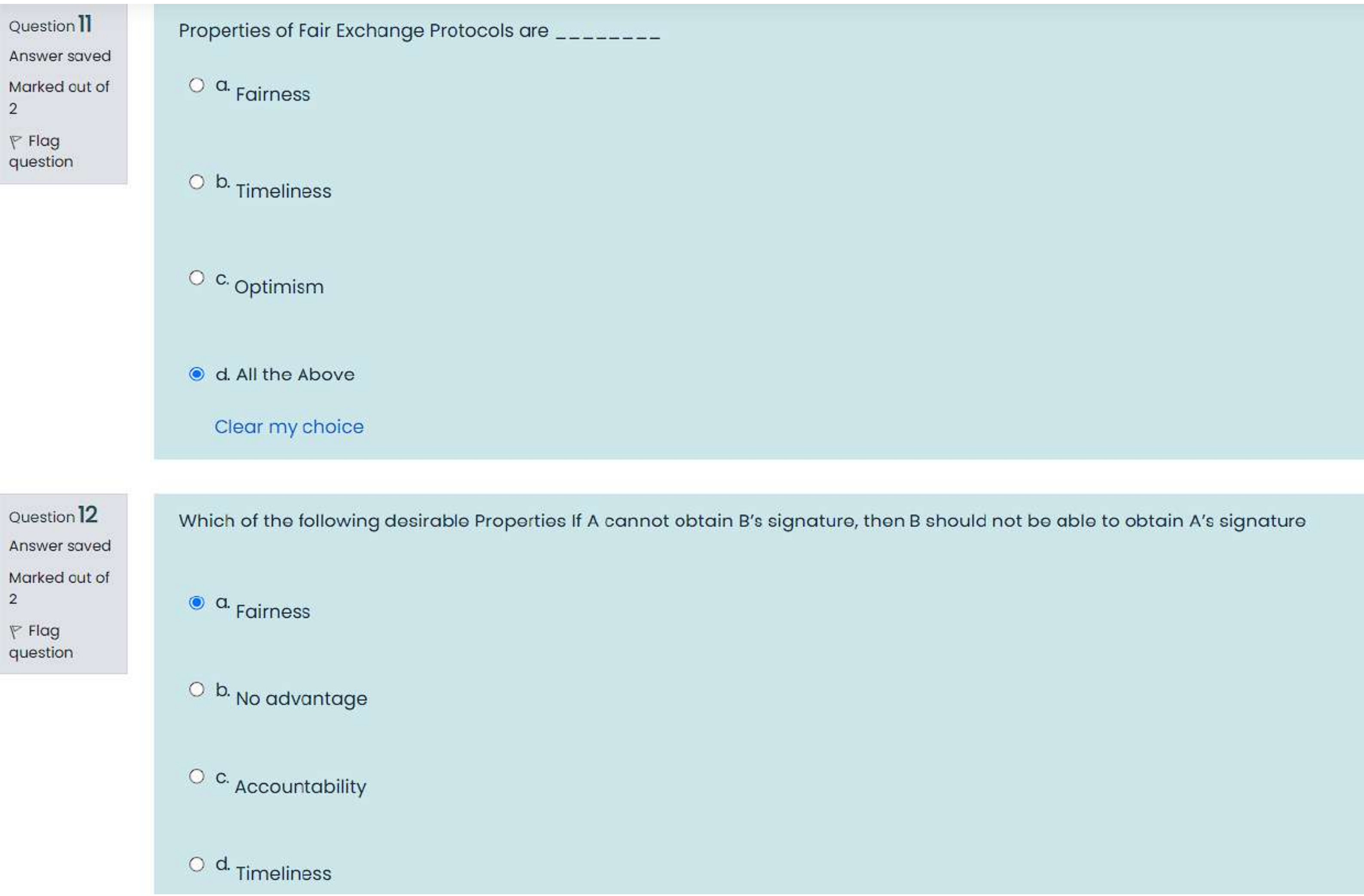
PCSX(m,Y,T) is an implementation of which of the following signature escrow

○ a. Ordinary and Verifiable Signature Escrows

○ b. None of them

○ c. Ordinary Signature Escrow

● d. Verifiable Signature Escrow



Question 11

Answer saved

Marked out of 2

Flag question

Properties of Fair Exchange Protocols are ________

○ a. Fairness

○ b. Timeliness

○ c. Optimism

● d. All the Above

Clear my choice

Question 12

Answer saved

Marked out of 2

Flag question

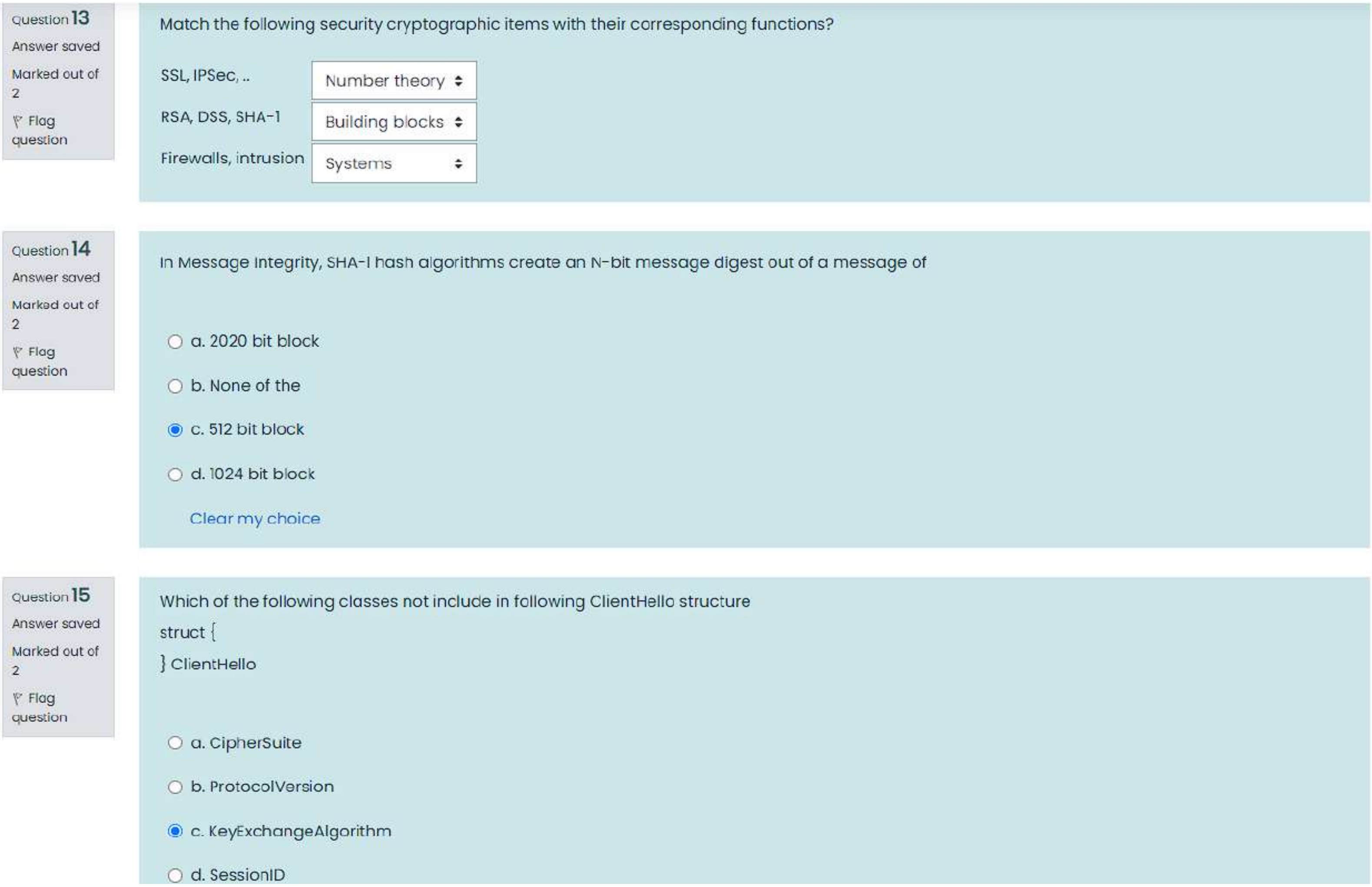
Which of the following desirable Properties If A cannot obtain B's signature, then B should not be able to obtain A's signature

● a. Fairness

○ b. No advantage

○ c. Accountability

○ d. Timeliness



Question 13
Answer saved
Marked out of 2
Flag question

Match the following security cryptographic items with their corresponding functions?

SSL, IPSec, ..	Number theory
RSA, DSS, SHA-1	Building blocks
Firewalls, intrusion	Systems

Question 14
Answer saved
Marked out of 2
Flag question

In Message Integrity, SHA-I hash algorithms create an N-bit message digest out of a message of

○ a. 2020 bit block

○ b. None of the

● c. 512 bit block

○ d. 1024 bit block

Clear my choice

Question 15
Answer saved
Marked out of 2
Flag question

Which of the following classes not include in following ClientHello structure

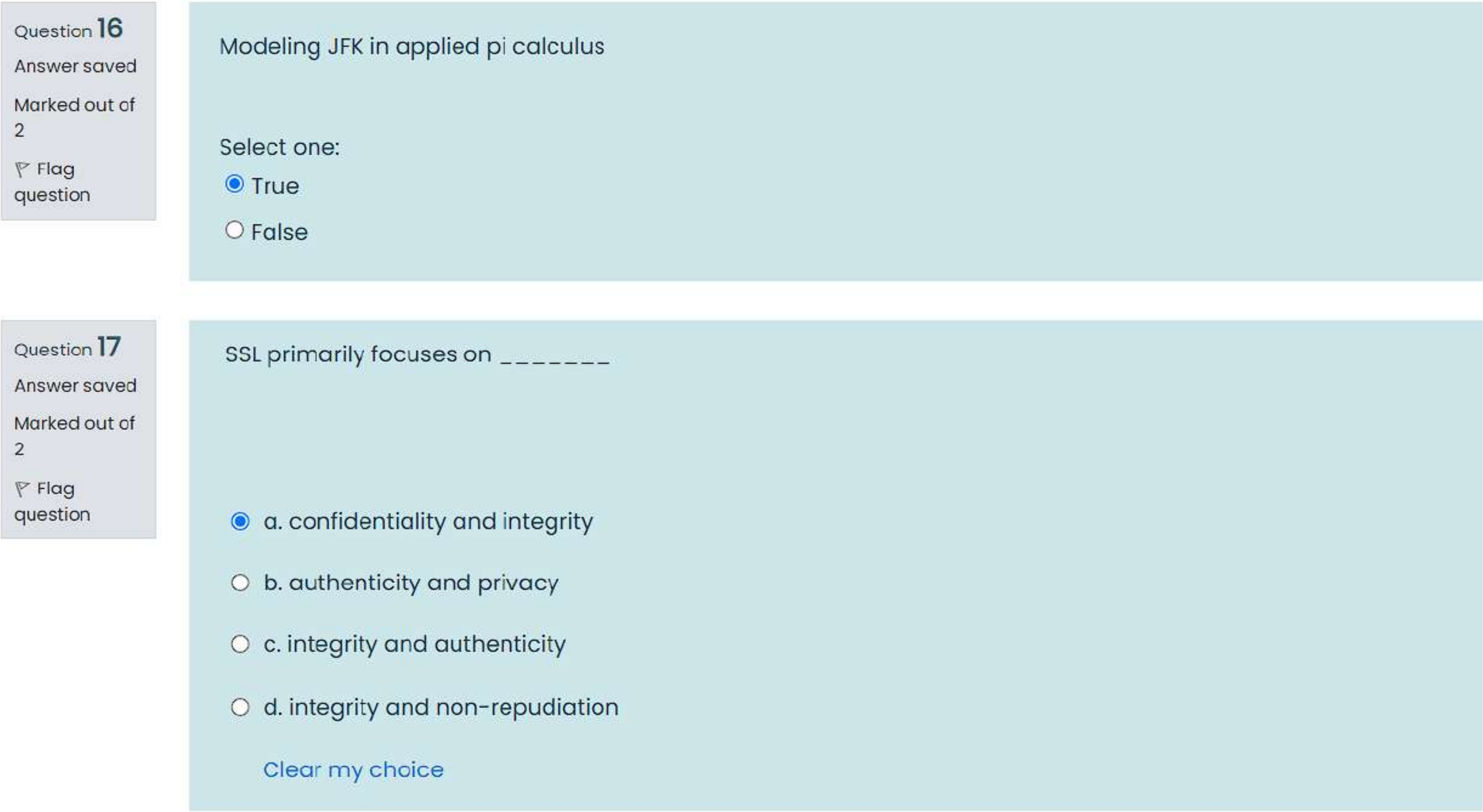
struct {
} ClientHello

○ a. CipherSuite

○ b. ProtocolVersion

● c. KeyExchangeAlgorithm

○ d. SessionID



Question 16

Answer saved

Marked out of 2

Flag question

Modeling JFK in applied pi calculus

Select one:

● True

○ False

Question 17

Answer saved

Marked out of 2

Flag question

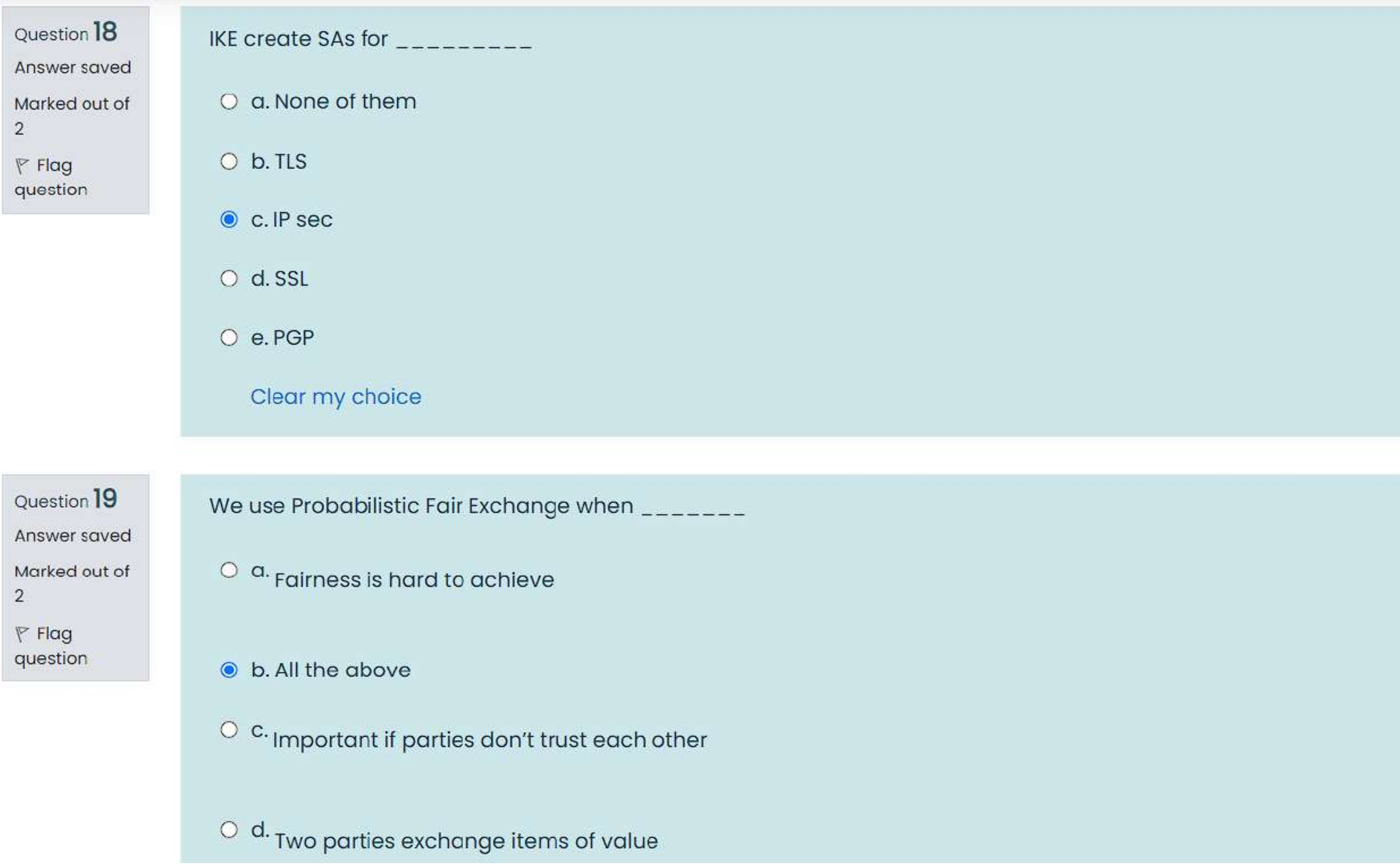
SSL primarily focuses on _______

● a. confidentiality and integrity

○ b. authenticity and privacy

○ c. integrity and authenticity

○ d. integrity and non-repudiation



Question 18

Answer saved

Marked out of 2

Flag question

IKE create SAs for _________

○ a. None of them

○ b. TLS

● c. IP sec

○ d. SSL

○ e. PGP

Clear my choice

Question 19

Answer saved

Marked out of 2

Flag question

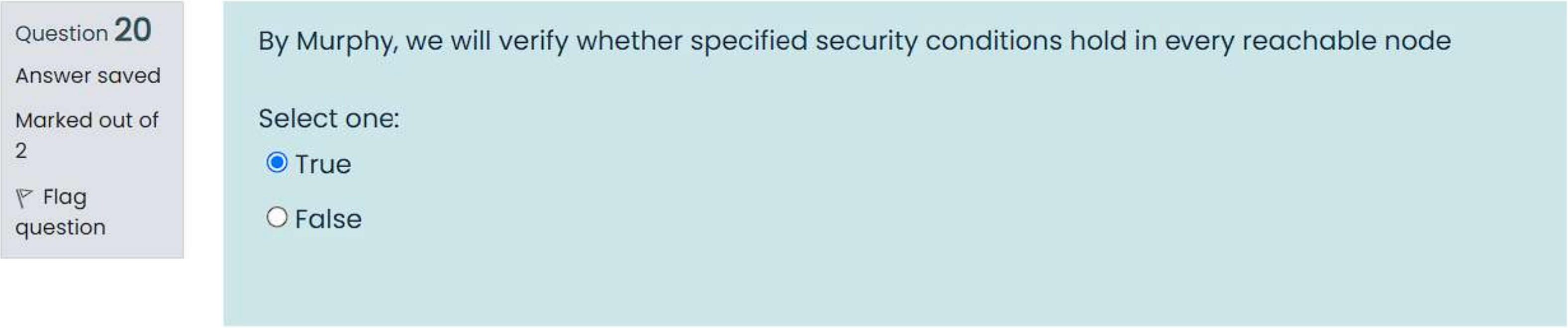
We use Probabilistic Fair Exchange when _______

○ a. Fairness is hard to achieve

● b. All the above

○ c. Important if parties don’t trust each other

○ d. Two parties exchange items of value



Question 20

Answer saved

Marked out of 2

Flag question

By Murphy, we will verify whether specified security conditions hold in every reachable node

Select one:

● True

○ False