Question 3

Answer saved

Marked out of 1

Flag question

The following procedure is Abort subprotocol

1- A Send to B PCSA(text,B,T)

2- B send to A PCSB(text,A,T)

3- A stop communicating

4- B send to TTP r1 = PCSA(text,B,T), sigB(text)

5- TTP send to B r2 = sigA(text) and store sigB(text)

Select one:

- True
- False

Question 4

Answer saved

Marked out of 1

Flag question

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

- a. Ordinary Signature Escrow
- b. Verifiable Signature Escrow
- c. None of them
- d. Ordinary and Verifiable Signature Escrows

Clear my choice

Question 5

Answer saved

Marked out of 1

Flag question

Every possible execution of the protocol is a path in protocol as a Game tree

Select one:

- True
- False

Question 6

Answer saved

Marked out of 1

Flag question

Which of the following role applied by TTP if one of the parties stops communicating, the other party can ask T to convert PCS into signature

- a. Abort Role
- b. Resolve and Abort Roles
- c. None of them
- d. Resolve Role

Question 7

Answer saved

Marked out of 1

Flag question

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

Select one:

- (●) True
- ( ) False

Question 8

Answer saved

Marked out of 1

Flag question

Which of the following desirable Properties no party from one side can determine the outcome

a. Accountability

b. No advantage

c. Timeliness

d. Fairness

Question 9

Answer saved

Marked out of 1

Flag question

The following procedure is ---------Escrows

- T can extract $sig_A(m)$ if formed correctly
- B can't extract $sig_A(m)$ but can verify that A's signature is inside and that T will be able to extract it

a. Ordinary escrow

b. Verifiable escrow

c. None of them

d. Ordinary escrow and Verifiable escrow

Clear my choice

Question 10

Answer saved

Marked out of 1

Flag question

Which of the following is/are type of contract signing Protocols?

- a. Probabilistic protocols
- b. Gradual-release protocols
- c. All the Above
- d. Fixed-round protocols with TTP

Question 1

Answer saved

Marked out of 1

Flag question

Define Properties on Game Trees: (Fairness)Property means no leaf node is labeled (Y,N) or (N,Y)

Select one:

- (●) True
- ( ) False

Question 2

Answer saved

Marked out of 1

Flag question

By the **Timeliness** desirable Property any party can terminate protocol by contacting TTP

Select one:

- (●) True
- ( ) False