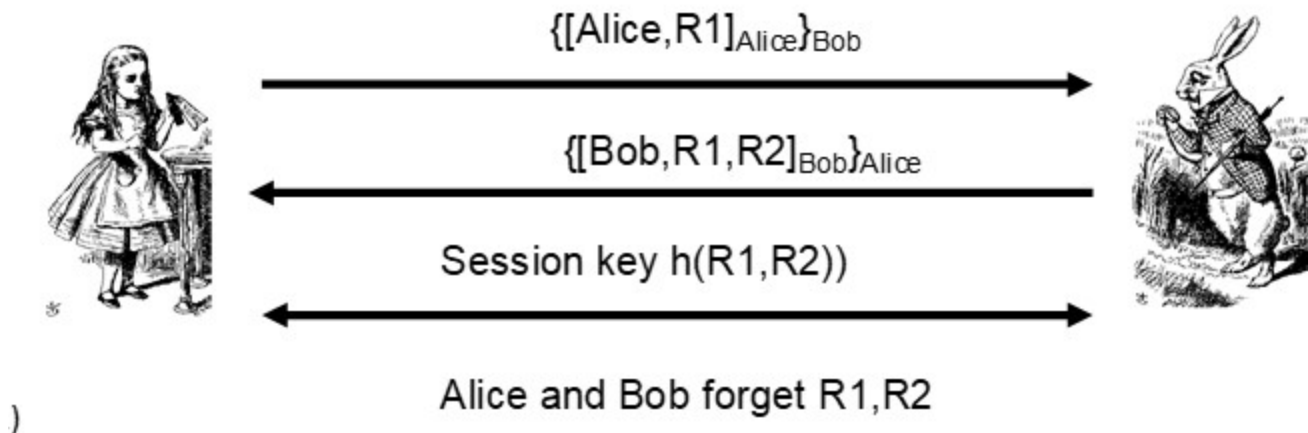


## Review Test Submission: Protocol self-quiz

User	Matthew LaChapelle
Course	Spring 2024 Computer Security (CS-492-01, CYS-492-01)
Test	Protocol self-quiz
Started	5/7/24 5:40 PM
Submitted	5/7/24 5:44 PM
Status	Completed
Attempt Score	20 out of 60 points
Time Elapsed	3 minutes
Results Displayed	All Answers, Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

## Question 1

10 out of 10 points



Is perfect forward secrecy between these two parties achieved?

Selected Answer: ☒ No

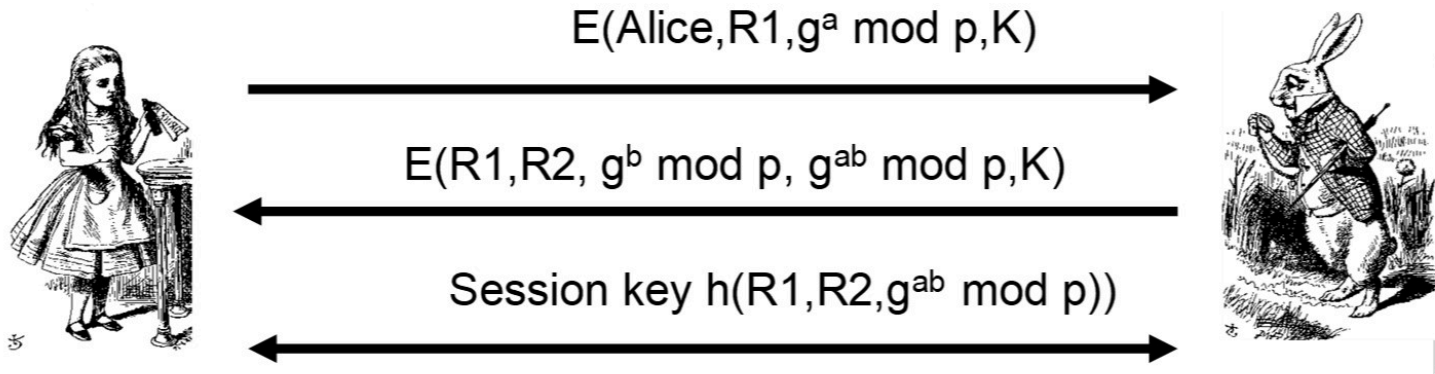
Answers: Yes

☒ No

Response Feedback: Correct

## Question 2

0 out of 10 points



After Alice and Bob forget  $R1, R2, a, \& b$

Where is Bob authenticated?

Selected Answer: ☒ No, Bob is never authenticated

Answers: Yes, by message 1

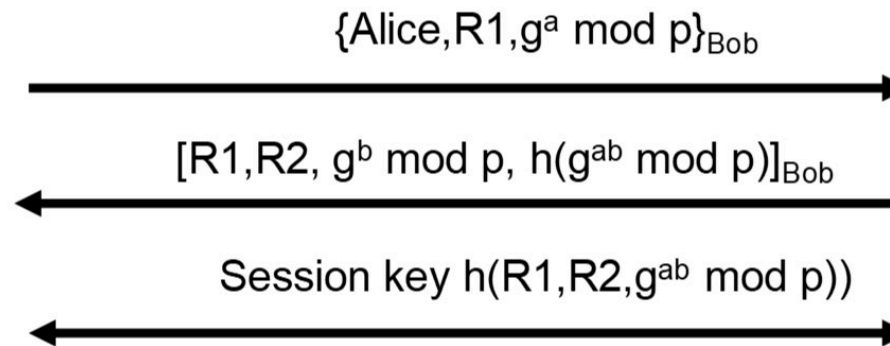
☒ Yes, by message 2

Yes, if he is able to send a message with the session key

No, Bob is never authenticated


## Question 3

0 out of 10 points




Alice and Bob forget  $R1$ ,  $R2$ ,  $a$  and  $b$

Where is Bob authenticated?

Selected Answer:  Yes, if he is able to send a message with the session key

Answers: Yes, by message 1

 Yes, by message 2

Yes, if he is able to send a message with the session key

No, Bob is never authenticated

## Question 4

10 out of 10 points



$$\{[Alice, R1]_{Alice}\}_{Bob}$$


$$\{[Bob, R1, R2]_{Bob}\}_{Alice}$$


Session key  $h(R1, R2)$



Alice and Bob forget  $R1, R2$

)

Is the session secure to a passive 3rd party?

Selected Answer: ☒ Yes

Answers: ☒ Yes

☐ No

Response Feedback: Correct

## Question 5

0 out of 10 points



$$\{Alice, R1, g^a \bmod p\}_{Bob}$$


$$[R1, R2, g^b \bmod p, h(g^{ab} \bmod p)]_{Bob}$$


$$\text{Session key } h(R1, R2, g^{ab} \bmod p)$$


Alice and Bob forget  $R1$ ,  $R2$ ,  $a$  and  $b$

Where is Alice authenticated?

Selected Answer: ☒ Yes, if she is able to send a message with the session key

Answers:

☐ Yes, by message 1

☐ Yes, by message 2

☐ Yes, if she is able to send a message with the session key

☒ No, Alice is never authenticated

## Question 6

0 out of 10 points



$$E(\text{Alice}, R1, g^a \bmod p, K)$$


$$E(R1, R2, g^b \bmod p, g^{ab} \bmod p, K)$$


$$\text{Session key } h(R1, R2, g^{ab} \bmod p)$$


After Alice and Bob forget  $R1, R2, a$ , &  $b$

Is perfect forward secrecy between these two parties achieved?

Selected Answer: ☒ Yes

Answers: ☐ Yes

☒ No

Response

Feedback:

No. If Trudy recorded this conversation and later recovered Alice and Bob's private keys she could recover everything to recreate the session key and decrypt the entire conversation.

Tuesday, May 7, 2024 5:44:04 PM EDT

← OK