# Security Quiz

**Due** May 10 at 7:20pm **Points** 50 **Questions** 8
**Available** after May 10 at 6:35pm **Time Limit** 45 Minutes

# Instructions

This quiz is timed for 45 minutes, and it has eight questions for the total of 50 points.

You may **not** use any text or notes, or any devices except what is required to access this quiz on Canvas. To enforce the Stevens Graduate Student Code of Integrity and Honor System, your video must be turned on so that everyone can see everyone else.

Unless you have been notified personally otherwise, you must submit your quiz no later than at 7:20 PM. Late submissions will not be accepted.

**Please make sure that you hit the submit button only once, or your answers might be lost!**

## Attempt History

| | Attempt | Time | Score |
|---|---|---|---|
| **LATEST** | Attempt 1 | 44 minutes | 50 out of 50 |

Score for this quiz: **50** out of 50
Submitted May 10 at 7:19pm
This attempt took 44 minutes.

### Question 1 — 5 / 5 pts

Using a symmetric cryptographic algorithm *S*, one can create a hash function *h(M)* using the technique called ____.

- Reflexion
- Encyphering

Encapsulation

Correct!

Digest

## Question 2

5 / 5 pts

Using a hash function that produces a 256-bit hash, one can encrypt a message of any length.

Correct!

True

False

## Question 3

5 / 5 pts

You and I share a key *K,* and you know that no one else can access this key. Using a symmetric-key encryption algorithm, *E,* I encrypt a message *M* and send the result, $E_K(M)$ to you. Can you be sure that I am the one who sent his message to you?

Correct!

True

False

## Question 4

5 / 5 pts

You and I share a key *K,* and you know that no one else can access this key. Using a symmetric-key encryption algorithm, *E,* I encrypt a message *M* and send the result, $E_K(M)$ to you. Can you prove that I am the one who had sent this message to you?

- True
- False

Correct!

## Question 5

10 / 10 pts

Alice and Bob share a key, *K,* and use the following authentication protocol in the network in which Trudy may both intercept and modify messages:

Alice Bob

---- A --->

<--- An even nonce *I* ---

----- $E_K(I)$ --->

<---- B ----

--- An odd nonce *J* -->

----- $E_K(J)$ --->

Can Trudy successfully stage a reflexion attack to impersonate either Alice or Bob?

- True
- False

Correct!

## Question 6

10 / 10 pts

**($A_{pu}$ , $A_{pr}$)** and **($B_{pu}$ , $B_{pr}$)** are, respectively, Alice's and Bob's **(public, private)** key pairs used for encryption and message signing.

Which, if any, is the correct way for Alice to send Bob a confidential message *M* so that Bob can prove that it came from Alice?

- $A_{pu}(A_{pr}(M))$
- $A_{pu}(B_{pr}(M))$

Correct!

- $B_{pu}(A_{pr}(M))$
- None of these

## Question 7

5 / 5 pts

**($A_{pu}$ , $A_{pr}$)** and **($B_{pu}$ , $B_{pr}$)** are, respectively, Alice's and Bob's **(public, private)** key pairs used for encryption and message signing. Which (if any) is a correct way to use these keys to respond to a challenge *C,* issued by Bob, to authenticate Alice?

- $B_{pu}(C)$
- $A_{pu}(C)$
- $A_{pr}(C)$

Correct!

- None of these

## Question 8

5 / 5 pts

A(n) _____ solves the problem of a user's VM key escrow to the Cloud provider.

- AWS Enterprise Key Escrow Service
- Trusted Platform Module (TPM)

Correct!

- Hardware Support Module (HSM)
- The OpenStack Keystone Module
- All items on this list

Quiz Score: **50** out of 50