Module 2 Quiz

Due Sep 6 at 11:59pm **Points** 5 **Questions** 5 **Time Limit** 30 Minutes

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	5 minutes	5 out of 5

Score for this quiz: **5** out of 5
Submitted Sep 3 at 8:06pm
This attempt took 5 minutes.

Question 1

1 / 1 pts

Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

- ○ True
- ◉ False

Correct!

Question 2

1 / 1 pts

The strength of a hash function against brute-force attacks depends solely on the length of the hash code produced by the algorithm.

Correct!

- (●) True
- ( ) False

Question 3

1 / 1 pts

The well-known symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the _____

- ( ) SHA
- ( ) RSA

Correct!

- (●) AES
- ( ) DSS

Question 4

1 / 1 pts

Which of these is considered as the most secure cryptographic hash function?

- MD5
- SHA1
- SHA-384
- SHA-512

Correct!

Question 5

1 / 1 pts

Based on the different schemes below, which is the least time-efficient scheme:

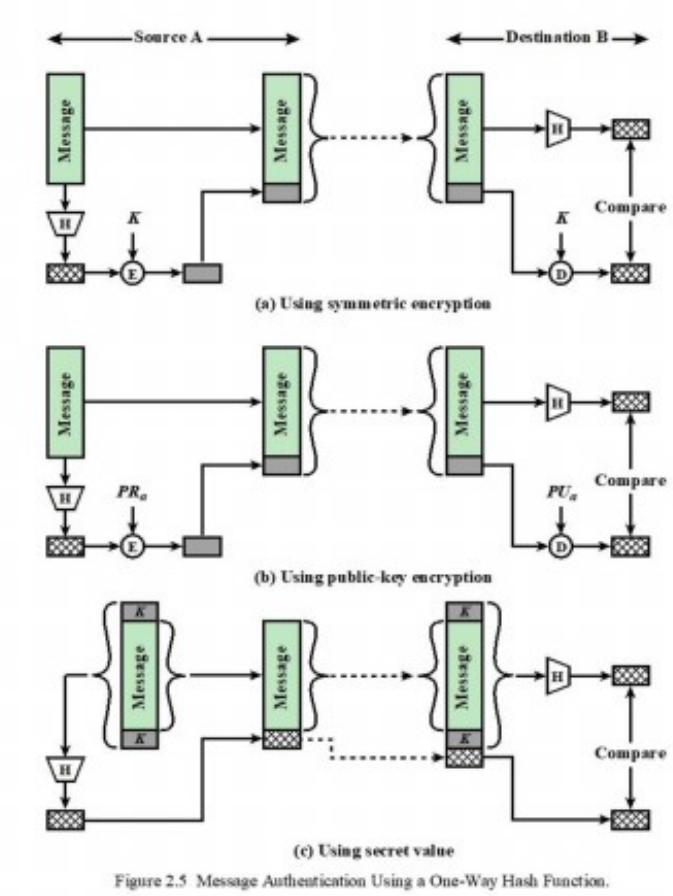

Figure 2.5 Message Authentication Using a One-Way Hash Function.

Correct!

- (●) Using public-key encryption
- ( ) Using symmetric key encryption
- ( ) Using secret value