Review Test Submission: Week 4 Module 1 Quiz (Click to start quiz)

User	Chad Chad Ballay
Course	CIS313-342N Cryptography (2203-DD)
Test	Week 4 Module 1 Quiz (Click to start quiz)
Started	12/9/19 10:56 AM
Submitted	12/9/19 11:04 AM
Status	Completed
Attempt Score	10 out of 10 points
Time Elapsed	8 minutes
Instructions	Select the best answer from the listed options.
Results Displayed	All Answers, Submitted Answers

Question 1

1 out of 1 points

Bob's password is hashed, and so is John's. Even though they used different passwords, the hash is the same. What is this called?

Selected Answer:	A collision
Answers:	A mistake
	Transposition
	Convergence
	A collision

Question 2

1 out of 1 points

A hashing method which can detect intentional alterations in a message is _____.

Selected Answer:	HMAC
Answers:	salt
	forensic integrity
	HMAC

checksum

Question 3 1 out of 1 points

According to your text, which hashing algorithm has known issues.

Selected Answer:	MD-5
Answers:	MD-5
	SHA-1
	SHA-2
	SHA-3

Question 4 1 out of 1 points

_____ is a 128-bit hash that is specified by RFC 1321 and was designed by Ron Rivest in 1991 to replace an earlier hash function.

Selected Answer:	MD5
Answers:	MD5
	RSA
	SHA-1
	SHA-256

Question 5 1 out of 1 points

In order to be a cryptographic hash function, an algorithm needs to have this property.

Selected Answer:	All of the above.
Answers:	The function must be one way.
	A variable-length input must produce a fixed-length output.
	There should be few or no collisions.
	All of the above.

Question 6

1 out of 1 points

Bob is looking for a cryptographic hash algorithm that needs to produce a 320-bit hash. Which of the following algorithms should he choose?

Selected Answer: RIPEMD

Answers: MD5

SHA-1

Tiger

SHA-3

RIPEMD

Question 7

1 out of 1 points

_____ is a cryptographic hash that can produce hashes of different lengths, and the user can specify the number of rounds used to produce the hash.

Selected Answer: HAVAL

Answers: SHA-3

Tiger

RIPEMD

HAVAL

Question 8

1 out of 1 points

Which hash algorithm is widely used in secure sockets layer, transport layer security, secure shell, and IPSEC?

Selected Answer: SHA-2

Answers: MD-5

SHA-1

SHA-2

SHA-3

Question 9

1 out of 1 points

Hashes are used to _____.

Selected Answer:	ensure integrity
Answers:	protect confidentiality
	maintain availability
	ensure integrity
	maintain integrity and confidentiality

Question 10

1 out of 1 points

In relationship to hashing, the term _____ refers to random bits that are used as one of the inputs to the hash. Essentially, the bits are intermixed with the message that is to be hashed.

Selected Answer:	salt
Answers:	vector
	stream
	IV
	salt

Monday, December 9, 2019 11:04:23 AM CST

← OK