Review Test Submission: Week 3 Quiz (Click to start Quiz)

User	Chad Chad Ballay
Course	CIS313-342N Cryptography (2203-DD)
Test	Week 3 Quiz (Click to start Quiz)
Started	12/7/19 10:22 AM
Submitted	12/7/19 10:30 AM
Status	Completed
Attempt Score	10 out of 10 points
Time Elapsed	7 minutes
Instructions	Select the best answer from the options given.
Results Displayed	All Answers, Submitted Answers

Question 1

1 out of 1 points

Which of the following was IBM's submission to the AES contest? This algorithm, one of the five finalists, uses a 128-bit block with key sizes between 128 and 448 bits.

Selected Answer: MARS

Answers: FEAL

Serpent

MARS

LOKI

Question 2

1 out of 1 points

Which of the following is a Feistel cipher?

Selected Answer: DES

Answers: AES

DES

RSA

RC4

Question 3

1 out of 1 points

Which of the following algorithms uses 33 subkeys or round keys, each 128 bits in size?

Selected Answer: Serpent

Answers: NESSIE

KHAZAD

AES

Serpent

Question 4

1 out of 1 points

_____ is a cipher invented by Vincent Rijmen and Paulo Barreto that uses eight rounds on a 64-bit block with a 128-bit key.

Selected Answer: Khazad

Answers: NESSIE

FISH

Shark

Khazad

Question 5

1 out of 1 points

_____ was designed by Martin Boesgaard, Mette Vetegrager, Thomas Pederson, Jesper Christiansen, and Ove Scavenis. It is a stream cipher that uses a 128-bit key along with a 64-bit initialization vector.

Selected Answer: Rabbit

Answers: NESSIE

Shark

FISH

Rabbit

Question 6 1 out of 1 points

How many rounds does DES have?

Selected Answer: 16

Answers: 56

16

4

64

Question 7 1 out of 1 points

_____ is a software-based stream cipher using a Lagged Fibonacci generator.

Selected Answer: FISH

Answers: Serpent

RC4

FISH

Shark

Question 8 1 out of 1 points

What algorithm does the clipper chip use?

Selected Answer: Skipjack

Answers: PIKE

Blowfish

Skipjack

Twofish

Question 9 1 out of 1 points

Which of the following is a symmetric key system using 64-bit blocks?

Selected Answer: DES

Answers: PGP

RSA

DES

Twofish

Question 10 1 out of 1 points

_____ was actually the forerunner to the Rijndael cipher. It was invented by Joan Daemen, Vincent Rijmen, and Lars Knudsen. It uses a 128-bit block with a 128-bit key working in eight rounds. This algorithm was first published in 1997.

Selected Answer: Square

Answers: NESSIE

Shark

Fish

Square

Sunday, December 8, 2019 4:44:25 PM CST

← **OK**