


CRYPTOGRAPHIC FUNDAMENTALS (BCSE2350 PR)

Question 1

Not yet answered

Marked out of 0.50

 Flag question

"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?


Select one:

- ☐ a. 128 key size: 10 rounds
- ☐ b. 192 key size: 12 rounds
- ☒ c. All of the above
- ☐ d. 256 key size: 14 rounds

[Clear my choice](#)**Question 2**

Not yet answered

Marked out of 0.50

 Flag question

Cipher block chaining or CBC is an advancement made on ____.


Select one:

- ☒ a. Electronic Code Book
- ☐ b. Decrypted code
- ☐ c. All of the mentioned above
- ☐ d. System engineering

[Clear my choice](#)**Question 3**

Not yet answered

Marked out of 0.50

 Flag question

In the AES-128 algorithm there are mainly _____ similar rounds and _____ round is different from other round.

Select one:

- ☐ a. 8 ; the first and last
- ☐ b. 10 ; no
- ☐ c. 5 similar rounds having 2 pair ; every alternate
- ☒ d. 9 ; the last

[Clear my choice](#)**Quiz navigation**

1	2	3	4	5	6	7	8	9
10								

[Finish attempt ...](#)Time left **0:14:09**

Search



Question 4

Not yet
answeredMarked out of
0.50

Flag question

Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher?

Select one:

- ☒ a. Both a. and b.
- ☐ b. None of the above
- ☐ c. Avalanche effect
- ☐ d. Completeness

[Clear my choice](#)

Question 5

Not yet
answeredMarked out of
0.50

Flag question

RSA algorithm is ____ cryptography algorithm.

Select one:

- ☐ a. Symmetric
- ☒ b. Asymmetric
- ☐ c. None of the mentioned above
- ☐ d. Systematic

[Clear my choice](#)

Question 6

Not yet
answeredMarked out of
0.50

Flag question

Amongst which of the following is / are true with reference to the rounds in AES –

Select one:

- ☐ a. Byte Substitution
- ☒ b. All of the mentioned above
- ☐ c. Mix Column and Key Addition
- ☐ d. Shift Row

[Clear my choice](#)

Question 7

Not yet

A secure block cipher is suitable for the encryption,




Search



[Clear my choice](#)

Question 7

Not yet
answeredMarked out of
0.50 Flag question


A secure block cipher is suitable for the encryption,

Select one:

- ☐ a. False
- ☒ b. True

[Clear my choice](#)

Question 8

Not yet
answeredMarked out of
0.50 Flag question


Using Rivest, Shamir, Adleman cryptosystem with $p=7$ and $q=9$. Encrypt $M=24$ to find ciphertext. The Ciphertext is:

Select one:

- ☐ a. 103
- ☐ b. 93
- ☐ c. 42
- ☒ d. 114

[Clear my choice](#)

Question 9

Not yet
answeredMarked out of
0.50 Flag question

When do we compare the AES with DES, which of the following functions from DES does not have an equivalent AES function in cryptography?

Select one:

- ☒ a. swapping of halves
- ☐ b. f function
- ☐ c. permutation p
- ☐ d. xor of subkey with function f

[Clear my choice](#)

Question 10

Not yet
answered

Cipher Feedback Mode is given as feedback to the ____ of encryption with some new specifications.



Search



0.50

Flag question

- ☐ b. 93
- ☐ c. 42
- ☒ d. 114

[Clear my choice](#)

Question 9

Not yet
answeredMarked out of
0.50

Flag question

When do we compare the AES with DES, which of the following functions from DES does not have an equivalent AES function in cryptography?

Select one:

- ☒ a. swapping of halves
- ☐ b. f function
- ☐ c. permutation p
- ☐ d. xor of subkey with function f

[Clear my choice](#)

Question 10

Not yet
answeredMarked out of
0.50

Flag question

Cipher Feedback Mode is given as feedback to the ____ of encryption with some new specifications.

Select one:

- ☒ a. Next block
- ☐ b. Middle block
- ☐ c. Previous block
- ☐ d. All of the mentioned above

[Clear my choice](#)

Finish attempt ...