Started on	Friday, 1 March 2024, 11:33 AM
State	Finished
Completed on	Friday, 1 March 2024, 11:53 AM
Time taken	20 mins 1 sec
Grade	**3.00** out of 9.00 (**33**%)

Question **1**

Incorrect

Mark 0.00 out of 1.00

MIXCOLUMN (32, 198, 201, 35) = ?

when we work on $\mathbb{F}_2[x]/ < x^8 + x^4 + x^3 + x^2 + 1 >$.

Input, output are in decimal.

a. (251, 212, 10, 41) ✖

b. (231, 18, 101, 55)

c. none of these

d. (253, 212, 12, 41)

e. (211, 213, 17, 37)

Your answer is incorrect.

The correct answer is:

(253, 212, 12, 41)

Question **2**

Correct

Mark 1.00 out of 1.00

Consider a Playfair cipher with key = aedoqmw

What is the correct ciphertext of the plaintext = iamd

- a. gdba ✔
- b. dgab
- c. hewe
- d. ehew
- e. none of these

Your answer is correct.

The correct answer is:
gdba

Question **3**

Correct

Mark 1.00 out of 1.00

Let p = 2147483647. If a = 13 then the multiplicative inverse

of a under mod p is =

- a. 1486719447
- b. 1486719448 ✔
- c. none of these
- d. 1486619448
- e. 1486729448

Your answer is correct.

The correct answer is:

1486719448

Question **4**

Incorrect

Mark 0.00 out of 1.00

MIXCOLUMN (32, 198, 201, 35) = ?

when we work on $\mathbb{F}_2[x]/ < x^8 + x^6 + x^5 + x^4 + x^2 + x + 1 >$.

Input, output are in decimal.

- a. (151, 212, 102, 41)
- b. (151, 212, 102, 11)
- c. none of these
- d. (151, 202, 102, 41)
- e. (151, 102, 212, 41) ✖

Your answer is incorrect.

The correct answer is:
(151, 212, 102, 41)

Question **5**

Not answered

Not graded

Consider a modified Playfair cipher on

{ A, B, C, D,..., Z, \ , /, [,] } . Note that the set has 30 elements.

Consider the key = AETIMPSB and select the encryption of

plaintext = CRYPTO\N

- a. QDUDWBEV
- b. QDUDBWEV
- c. QDUDBWVE
- d. none of these
- e. QDDUBWEV

Your answer is incorrect.

The correct answers are:
QDUDBWEV,

none of these

Question **6**

Incorrect

Mark 0.00 out of 1.00

Consider AES-Subbyte table Sub().

We define a new S-box from Sub as follows:

S(x) = Sub((2*x)+1), here a*x and y+b are done in

$\mathbb{F}_2[x]/ < x^8 + x^6 + x^5 + x^4 + x^2 + x + 1 >$.

What is value of S(212)? Here input, output are in decimal.

- a. 113
- b. 29
- c. 92 ✖
- d. 28
- e. none of these

Your answer is incorrect.

The correct answer is:
29

Question **7**

Correct

Mark 1.00 out of 1.00

CAESAR-Encryption (aeqwg) = ?

- a. dthjz
- b. dhtzq
- c. dhtzj ✔
- d. none of these
- e. ahtzj

Your answer is correct.

The correct answer is:
dhtzj

Question **8**

Incorrect

Mark 0.00 out of 1.00

Consider Affine encryption algorithm.

If the secret key is K = (11,5), the ciphertext of the

plaintext = aeswq is = ?

- a. fxvnz
- b. none of these
- c. fxvny ✖
- d. fzvnx
- e. fxnvz

Your answer is incorrect.

The correct answer is:
fxvnz

Question **9**

Incorrect

Mark 0.00 out of 1.00

Consider AES-Subbyte table Sub().

We define a new S-box from Sub as follows:

S(x) = Sub((2*x)+1), here a*x and y+b are done in

$\mathbb{F}_2[x]/ < x^8 + x^4 + x^3 + x + 1 >$.

What is value of S(126)? Here input, output are in decimal.

- a. 48
- b. 84
- c. 83
- d. 88 ✖
- e. none of these

Your answer is incorrect.

The correct answer is:
84

Question **10**

Incorrect

Mark 0.00 out of 1.00

Consider Shift cipher and find the encryption of

the plaintext = aeqwg

where key = 5

- a. fjvlb
- b. none of these
- c. fjvbl
- d. fvjbl ✖
- e. fjvbp

Your answer is incorrect.

The correct answer is:
fjvbl

◄ Announcements

Jump to...

LAB -Assignment 1 ►