Started on	Friday, 1 March 2024, 11:03 AM
State	Finished
Completed on	Friday, 1 March 2024, 11:23 AM
Time taken	20 mins 3 secs
Grade	**5.50** out of 6.00 (**92**%)

Question **1**

Correct

Mark 0.50 out of 0.50

Which is the correct multiplicative inverse of the polynomial $g(x)=x^3+x^2$ in $Z_2[x]/x^8+x^4+x^3+x+1$.

a. x^3+x+1

b. x^6+x^3+x

c. $x^7+x^5+x^4$ ✔

Your answer is correct.

The correct answer is:

$x^7+x^5+x^4$

Question **2**

Correct

Mark 0.50 out of 0.50

What is the period of the 5-bit LFSR whose connection polynomial is $x^5 + x^4 + x^2 + x + 1$

- a. 32
- b. 31 ✔
- c. 16
- d. none of these
- e. 15

Your answer is correct.

The correct answer is:
31

Question **3**

Correct

Mark 0.50 out of 0.50

A sequence of plaintext blocks x1,...,xn are encrypted by

using AES-128 in CBC mode. The corresponding ciphertext blocks

are y1,...,yn. During transmission y1 is transmitted incorrectly

(i.e., some 1's are changed to 0's and vice verse).

The number of plaintext blocks that will be decrypted incorrectly is

a. 1

b. n

c. 3

d. none of these

e. 2 ✔

Your answer is correct.

The correct answer is:

2

Question **4**

Correct

Mark 0.50 out of 0.50

Which is the correct multiplicative inverse of the polynomial $g(x) = x^3 + x^2$ in $\mathbb{Z}_2[x]/x^5 + x^4 + x^2 + x + 1$.

a. $x^4 + x^2 + x + 1$

b. $x^4 + x^3 + x^2 + x + 1$ ✔

c. $x^4 + x^3 + x$

Your answer is correct.

The correct answer is:

x^4 + x^3 + x^2 + x + 1

Question **5**

Correct

Mark 0.50 out of 0.50

Consider one-bit encryption $C=P\oplus K$. If $Pr[K=0]=0.5$ and $Pr[P=1]=0.3$

then $Pr[P=0|C=1]$ is

a. 0.3

b. 0.4

c. 0.7 ✔

d. none of these

e. 0.5

Your answer is correct.

The correct answer is:

0.7

Question **6**

Correct

Mark 1.00 out of 1.00

If AES-Mixcolumn(23, 67, 89, 45) = (x,y,z,w) then w =

[here input and output are in integer]

a. none of these

b. 87

c. 121 ✔

d. 145

e. 159

Your answer is correct.

The correct answer is:

121

Question **7**

Incorrect

Mark 0.00 out of 0.50

Select the correct answer where S_1: $\{0,1\}^6 \rightarrow \{0,1\}^4$ and S_2:$\{0,1\}^6 \rightarrow \{0,1\}^4$ are the first two

defined S-boxes for the round function of DES. (For the description of these S-boxes please

see Handbook of Applied Cryptography book.)

a. $S_1(59) = 0, S_2(23) = 10.$

b. $S_1(59) = 4, S_2(23) = 8$ ✖

c. $S_1(59) = 1, S_2(23) = 10.$

d. $S_1(59) = 0, S_2(23) = 14.$

Your answer is incorrect.

The correct answer is:
$S_1(59) = 0, S_2(23) = 10.$

Question **8**

Correct

Mark 1.00 out of 1.00

If AES-Mixcolumn(23, 67, 45, 89) = (x,y,z,w) then y =

[here input and output are in integer]

a. 191 ✔

b. 121

c. 159

d. 229

Your answer is correct.

The correct answer is:

191

Question **9**

Correct

Mark 0.50 out of 0.50

We define a new encryption algorithm TEnc using AES-128 encryption

technique.

TEnc : $\{0,1\}^{384}\times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ where

C = TEnc(K||K1||K2, M) = K2 $\oplus$ AES-128-Enc(K, K1 $\oplus$ M).

Here K, K1, K2 each is of 128 bit. What will be the decryption algorithm

(TDec) corresponding to TEnc.

a. M = TDec(K||K1||K2, C) = K2 $\oplus$ AES-128-Dec(K, K1 $\oplus$ C)

b. M = TDec(K||K1||K2, C) = K1 $\oplus$ AES-128-Dec(K, K2 $\oplus$ C) ✔

c. None of these

d. M = TDec(K||K1||K2, C) = K \oplus AES-128-Dec(K1, K2 \oplus C)

Your answer is correct.

The correct answer is:

M = TDec(K||K1||K2, C) = K1 \oplus AES-128-Dec(K, K2 \oplus C)

Question **10**

Correct

Mark 0.50 out of 0.50

Consider AES-256 bit encryption algorithm and a 512 bit key K=K1||K2 where K1 and K2 are of 256 bit.

The encryption algorithm C=AES-256(AES-256(M,K1),K2) provides

a. 512-bit security

b. 256-bit security ✔

Your answer is correct.

The correct answer is:

256-bit security

◄ Announcements

Jump to...

Midterm ►