Assignment 3

The due date for submitting this assignment has passed. As per our records you have not submitted this assignment.

Due on 2019-02-20, 23:59 IST

1) While defining finite extension fields with irreducible polynomials

a. Degree of the irreducible polynomial should be equal to the logarithm of the order of the field.
b. Degree of the irreducible polynomial should be greater than the logarithm of order of the field
c. Degree of the irreducible polynomial should be lesser than the logarithm of order of the field
d. No such relationship exists

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

2) To represent a finite field

a. The irreducible polynomial must be primitive polynomial
b. The irreducible polynomial may not be primitive polynomial
c. You do not need primitive polynomial
d. None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
During the computation of the MixColumns matrix of AES in finite field of $GF((2^4)^2)$ we can have:

a. $T(3)(\alpha_1 x + \alpha_0) = T(2)(\alpha_1 x + \alpha_0) + (\alpha_1 x + \alpha_0)$

b. $T(3)(\alpha_1 x + \alpha_0) = T(1)(\alpha_1 x + \alpha_0) + (\alpha_1 x + \alpha_0)$

c. $T(3)(\alpha_1 x + \alpha_0) = T(2)(\alpha_0 x + \alpha_1) + (\alpha_1 x + \alpha_0)$

d. None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

4) Inversion-MixColumns can be computed by reusing the MixColumns matrix. The lightweight ways of doing are:

[Multiple answers may be correct]

a. Adding MixColumn matrix with two other constant matrices

b. Multiplying MixColumn matrix with two other constant matrices

c. Taking an inverse of the MixColumn matrix

d. None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

5) A normal basis for $GF((2^8)^2)$ where $\alpha$ is a root of the primitive polynomial $p(x)$ over $GF((2^8)^2)$ is

a. $\{\alpha, \alpha^{16}\}$

b. $\{\alpha, \alpha^{32}\}$

c. $\{\alpha, \alpha^4\}$

d. $\{\alpha, \alpha^{6}\}$

No, the answer is incorrect.
Score: 0
Accepted Answers:
b.
We construct the isomorphic mapping between $GF(2^4)$ and $GF(2^2)^2)$. The primitive polynomials considered are:

- I. For $GF(2^4): R(Z) = Z^4 + Z^3 + 1$
- II. For $GF(2^3): Q(Y) = Y^2 + Y + 1$
- III. For $GF((2^2)^2)): P(X) = X^2 + X + [2]$

Based on the above information answer the following question.

The primitive element $\gamma$ in $GF(2^4)$ is:

- a. 02
- b. 04
- c. 11
- d. 09

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

The mapping, discussed in Question 6, can be defined by finding another primitive polynomial element $\alpha \in GF((2^3)^2)$ for which:

- a. $R(\alpha) \equiv 0 \mod Q(Y)P(X)$
- b. $R(\alpha) \equiv 1 \mod Q(Y)P(X)$
- c. $R(\alpha) \equiv \gamma \mod Q(Y)P(X)$
- d. None of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
a.

What should be the value of $\alpha$ in Question 7?

- a. 04
- b. 08
- c. 06
- d. 09

No, the answer is incorrect.
Score: 0
Accepted Answers:
d.
9) Consider the Affine Transformation matrix of AES S-Box. Let us denote it by $A$. After transferring it to composite field, we have $A' = TAT^{-1}$ where $T$ is the matrix defining the isomorphism mapping. Depending on the choice of $T$ the hardware complexity of affine transformation may vary. Consider the two following matrices as two alternatives of $A'$

\[
\begin{align*}
\text{Choice 1: } A' &= \begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{pmatrix} \\
\text{Choice 2: } A' &= \begin{pmatrix}
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{pmatrix}
\end{align*}
\]

The number of XOR gates required for the first choice:

a. 21  
b. 40  
c. 64  
d. 32

No, the answer is incorrect.  
Score: 0  
Accepted Answers: c.

10) The number of XOR gates required for second choice, as given in Question 9, is

a. 40  
b. 32  
c. 10  
d. 18

No, the answer is incorrect.  
Score: 0  
Accepted Answers: c.