X

reviewer2@nptel.iitm.ac.in ▼

Courses » Introduction To Cryptology

Announcements **Course** Ask a Question Progress

Unit 3 - Week 2

Course outline

How to access the portal?

Week 1

Week 2

- ○ Lecture 1: Product Ciphers and Block Ciphers
- ○ Lecture 2: Substitution-Permutation Network and Feistel Cipher
- ○ Lecture 3: S-box Theory
- ○ Lecture 4: Cryptanalysis of Block Ciphers
- ○ Lecture 5: Problem discussions from Week – 1
- ○ Quiz : Week2_Assignment1
- ○ Assignment Solution
- ○ Feedback form for Week-2

Week 3

Week 4

Week2_Assignment1

The due date for submitting this assignment has passed. **Due on 2017-08-09, 23:59 IST.**
As per our records you have not submitted this assignment.

1) Let S_1 be a multiplicative cipher over Z_{26} and S_2 be a shift cipher over Z_{26}. Suppose that $S = S_1 \times S_2$. Find the ciphertext y of "JULIUS“ using the cryptosystem S, where k_1 = 3 and k_2 = 11, is. ***1 point***

○ y=MTSJTM
○ y= MTSJTN
○ y= PTSJTN
○ y= QTSJTN

No, the answer is incorrect.
Score: 0

Accepted Answers:
y= MTSJTN

2) Suppose S_1 and S_2 are Vigenere Ciphers with keyword length m_1 and m_2, respectively, where $m_2 \mid m_1$.Then determine which of the following statement is correct. ***1 point***

○ $S_1 \times S_2 = S_2$.
○ $S_2 \times S_1 = S_1$.
○ $S_2 \times S_1 = S_2$.
○ None of the above.

No, the answer is incorrect.
Score: 0

Accepted Answers:
$S_2 \times S_1 = S_1$.

3) Let $\pi(x_1, x_2, x_3, x_4) = (x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)})$ be the permutation on a SPN network, where ***1 point***

i	1	2	3	4
π(i)	2	4	1	3

and the 4×4 S-box function be

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	3	5	7	9	B	D	F	E	C	A	8	6	4	0	2

If x = 1101, then determine the correct statement.

○ S(π(x))= 0000.
○ S(π(x))= 1110.
○ S(π(x))= 0001.
○ S(π(x))= 1111.

No, the answer is incorrect.
Score: 0

Accepted Answers:

$S(\pi(x)) = 0000$.

4) Let y = 10101110 be the output of a Feistel cipher of length 8 applying one round with key k = 0110 and let the key mixing function be $f(x,k)$ = S($x \oplus k$) where S is defined using following table. ***1 point***

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	1	3	5	7	9	B	D	F	E	C	A	8	6	4	0	2

Which is the following input is correct?

○ 0001 1010
○ 1010 0001
○ 1010 1000
○ 1000 1010

No, the answer is incorrect.
Score: 0

Accepted Answers:
1000 1010

5) Let $f(x_3, x_2, x_1) : GF(2)^3 \rightarrow GF(2)$ be a Boolean function such that (f(0,0,0), f(0,0,1),…, f(1,1,1)) = (0, 0, 0, 1, 1, 1, 1, 0).Then the algebraic normal form of f is ***1 point***

○ $x_1x_2 \oplus x_3$.
○ $x_1x_3 \oplus x_2$.
○ $x_3x_2 \oplus x_1$.
○ $x_1x_2 \oplus x_3x_4$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
$x_1x_2 \oplus x_3$.

6) Let $f : GF(2)^3 \rightarrow GF(2)$ and $g : GF(2)^3 \rightarrow GF(2)$ be two Boolean functions such that (f(000), f(001),..., f(111)) = (1, 0, 1, 0, 1, 1, 1, 1) and (g(000), g(001),..., g(111)) = (0, 1, 0, 1, 1, 0, 1, 1). Then the Hamming weight between two functions f and g is ***1 point***

○ 4
○ 5
○ 3
○ 6

No, the answer is incorrect.
Score: 0

Accepted Answers:
5

7) Let $f : GF(2)^2 \rightarrow GF(2)$ be a Boolean function such that $f(x_1,x_2) = x_1x_2 \oplus x_1$. Suppose that $nl(f)$ be the nonlinearity of f and $d(f)$ be the maximum distance from all affine functions of 2 variables. Then ***1 point***

○ $nl(f)$ = 1, $d(f)$ = 2
○ $nl(f)$ = 1, $d(f)$ = 3
○ $nl(f)$ = 2, $d(f)$ = 3
○ $nl(f)$ = 2, $d(f)$ = 2

No, the answer is incorrect.
Score: 0

Accepted Answers:
$nl(f)$ = 1, $d(f)$ = 3

8) Let F: $GF(2)^2 \rightarrow GF(2)^2$ be a 2×2 S-box function such that $F(x_1,x_2) = (x_1x_2 \oplus x_1, x_1x_2 \oplus x_2)$ ***1 point***

Then the nonlinearity of F is

○ 1
○ 3
○ 2
○ 0

No, the answer is incorrect.
Score: 0

Accepted Answers:
0

9) Suppose that we have two plaintext and ciphertext pairs obtained from Affine cipher (8,0) and (4,14) over Z_{26}. Find the value of a and b, where $k = (a,b)$ is a key. ***1 po***

○ $a = 2$, $b = 3$.
○ $a = 2$, $b = 2$.
○ $a = 3$, $b = 2$.
○ $a = 3$, $b = 3$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
$a = 3$, $b = 2$.

10)Let F: $GF(2)^4 \rightarrow GF(2)^3$ be a 4×3 S-box function of a block cipher such that $F(x_1,x_2,x_3,x_4)$= (y_1,y_2,y_3), where $y_1 = x_1x_2x_3 \oplus x_3x_4 \oplus x_1 \oplus x_2$, $y_2 = x_1x_2x_3 \oplus x_3x_4 \oplus x_2$ and $y_3 = x_1 \oplus x_2 \oplus x_4 \oplus 1$. We consider single round of the block cipher with key $k = (k_1, k_2, k_3, k_4)$ is xored bitwise to the plaintext bits before obtaining the output by applying F. ***1 point***

Which following relations is valid?

○ $k_1 = x_1 \oplus y_1 \oplus y_2$ and $k_2 \oplus k_4 = 1 \oplus x_2 \oplus y_1 \oplus y_2 \oplus y_3$
○ $k_1 = x_1 \oplus y_2$ and $k_2 \oplus k_4 = 1 \oplus x_2 \oplus x_4 \oplus y_1 \oplus y_2 \oplus y_3$
○ $k_1 = x_1 \oplus y_1 \oplus y_2$ and $k_2 \oplus k_4 = 1 \oplus x_2 \oplus x_4 \oplus y_1 \oplus y_2 \oplus y_3$
○ $k_1 = x_1 \oplus y_1 \oplus y_2$ and $k_2 \oplus k_4 = 1 \oplus x_2 \oplus x_3 \oplus y_1 \oplus y_2 \oplus y_3$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$k_1 = x_1 \oplus y_1 \oplus y_2$ and $k_2 \oplus k_4 = 1 \oplus x_2 \oplus x_4 \oplus y_1 \oplus y_2 \oplus y_3$

Previous Page

End