Unit 4 - Week 2

Course outline

How does an NPTEL online course work?

Week 0 Assignment 0

Week 1

Week 2

- Lecture 6: Data Encryption Standard (DES)
- Lecture 7: Data Encryption Standard (DES) (Contd.)
- Lecture 8: Triple DES and Modes of Operation
- Lecture 9: Stream Cipher
- Lecture 10: Pseudorandom Sequence
- Lecture material of Week 2
- Quiz : Week 2 Assignment 2
- Week 2 Feedback Form

Week 3

Week 4

Week 5

Week 6

Week 7

Week 8

Week 9

Week 10

Week 11

Week 12

Download Videos

Detail Solution

Text Transcripts

Week 2 Assignment 2

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

Due on 2020-02-12, 23:59 IST.

1) What kind of cipher DES is? 1 point

A. Stream cipher
B. Block cipher
C. Bit cipher
D. Permutation cipher

A.
B.
C.
D.

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

2) How many rounds of Feistel cipher are used in DES encryption scheme? 1 point

A. 8
B. 14
C. 18
D. 16

A.
B.
C.
D.

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

3) Total number of s-box used in DES encryption algorithm is _____. 1 point

A. 8
B. 6
C. 4
D. 16

A.
B.
C.
D.

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

4) 1 point

In one round of DES encryption algorithm the complex function 'F' produces an output of length _____ bits.

A. 48
B. 64
C. 57
D. 32

A.
B.
C.
D.

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

5) The only difference between DES encryption and DES decryption algorithm is in _____. 1 point

A. number of feistel rounds
B. complex function 'F'
C. permutation tables
D. key scheduling algorithm

A.
B.
C.
D.

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

6) 1 point

Let *Block* be a block cipher consisting of two rounds of a feistel cipher having block length 8 with the session keys k_1, k_2 such that $k = k_1||k_2$ be the secret key. Suppose the complex function F used in the feistel cipher is simple XOR with the session key. That is, $F(m', k') = m' \oplus k'$ for input string m' and session key k'. Find the ciphertext $Block(m, k)$ where the message $m = 10100101$ and the secret key $k = 11001010$.

A. 11111111
B. 00111100
C. 10111100
D. 00110011

A.
B.
C.
D.

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

7) Triple DES algorithm uses _____ different keys each of size 64-bit. 1 point

A. 3
B. 4
C. 5
D. 2

A.
B.
C.
D.

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

8) Which of the following statements is(are) true? 1 point

(i) Block Ciphers can not reuse a particular key for many encryptions.
(ii) Stream Ciphers are fasters than Block Ciphers.

A. only (i)
B. only (ii)
C. neither (i) nor (ii)
D. both (i), (ii)

A.
B.
C.
D.

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

9) Which of the following cryptosystems, if implemented properly, is impenetrable? 1 point

A. Substitution Cryptosystem
B. Vigenere Cryptosystem
C. Enigma Cryptosystem
D. One-time pad

A.
B.
C.
D.

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

10) 1 point

Consider one-bit encryption $C = P \bigoplus K$ with $\Pr(K = 0) = 0.5$ and $\Pr(P = 1) = 0.3$ then $\Pr(P = 0|C = 1)$ is

A. 0.7
B. 0.3
C. 0.4
D. 0.5

A.
B.
C.
D.

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