X

NPTEL

reviewer3@nptel.iitm.ac.in ▾

Courses » Information Theory, Coding and Cryptography

Announcements **Course** Ask a Question Progress Mentor FAQ

Unit 13 - Week 12

Course outline

How to access the portal

Week 1

Week 2

Week 3

Week 4

Week 5

Week 6

Week 7

Week 8

Week 9

Week 10

Week 11

Week 12

○ Introduction to Cryptography : Symmetric Key and Asymmetric Key Cryptography

○ Some

Assignment 12

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

Due on 2018-10-24, 23:59 IST.

1) The number of one-to-one affine ciphers that can be constructed for the English alphabet is ***1 point***

○ 255

○ 312

○ 512

○ 616

No, the answer is incorrect.
Score: 0

Accepted Answers:
312

2) The total number of unique keys possible for the Playfair cipher (including the trivial cases) is approximately given by ***1 point***

○ 2^{24}

○ 2^{64}

○ 2^{84}

○ 2^{104}

No, the answer is incorrect.
Score: 0

Accepted Answers:
2^{84}

3) Consider RC4 with the internal state, S, and the two indices i and j. The number of internal states are ***1 point***

○ 2^{1700}

A project of

NPTEL National Programme on Technology Enhanced Learning

In association with

NASSCOM®

Funded by

Additional Lectures

ce De

Accepted Answers:
2^{1700}

4) If we use the prime numbers 29 and 61 to generate keys using the RSA algorithm, then a possible choice of the public key could be ***1 point***

○ 7
○ 9
○ 11
○ 13

No, the answer is incorrect.
Score: 0

Accepted Answers:
11

5) The ciphertext obtained for message M = 2 when using RSA to perform encryption with A = 17, B = 31 and public key E = 7 is ***1 point***

○ 64
○ 128
○ 162
○ 212

No, the answer is incorrect.
Score: 0

Accepted Answers:
128

6) Suppose A and B use the Diffie-Hellman key exchange protocol with a common prime P = 71 and the primitive root = 7.If user A has private key K_A= 5 and user B has private key K_B= 12, then the shared secret key is ***1 point***

○ 30
○ 32
○ 40
○ 42

No, the answer is incorrect.
Score: 0

Accepted Answers:
30

7) Suppose the point (a,7) lies on the elliptic curve y^2= x^3 + 11x + 19 (mod 167), then the value of a is ***1 point***

○ 0
○ 1
○ 2
○ 4

No, the answer is incorrect.
Score: 0

Accepted Answers:
2

8) Suppose we want to test the security of character + x encrypting technique in which each ***1 point***

alphabet of the plaintext is shifted by x to produce the ciphertext. Assuming it takes a computer 1 ms to check out one value of the shift, how soon can this code be broken

○ 20 ms

○ 25 ms

○ 35 ms

○ 40 ms

No, the answer is incorrect.
Score: 0

Accepted Answers:
25 ms

9) Upon decoding the Vigenère ciphertext:QQNLMEPQBVLBI using the key ' IIT ' we obtain the plaintext as ***1 point***

○ IITDELHIINDIA

○ IITPATNABIHAR

○ NITKURUKSHETRA

○ IITMANDIINDIA

No, the answer is incorrect.
Score: 0

Accepted Answers:
IITDELHIINDIA

10)Consider the elliptic curve given by E: $y^2 = x^3 + 17$ over the real number field with points P = (– 1, 4) and Q = (2, 5) ∈ E. Then,P – Q is given by ***1 point***

○ (3, 27)

○ (8, 23)

○ (4, 19)

○ (18, 3)

No, the answer is incorrect.
Score: 0

Accepted Answers:
(8, 23)

Previous Page End