

X

NPTEL

reviewer2@nptel.iitm.ac.in ▼

Courses » Introduction To Cryptology

Announcements

Course

Ask a Question

Progress



Unit 4 - Week 3

Course outline

How to access the portal?

Week 1

Week 2

Week 3

- Lecture 1: Public-Key Cryptography
- Lecture 2: RSA Computation
- Lecture 3: Primality Testing-1
- Lecture 4: Primality Testing-2
- Lecture 5: Problem Discussions
- Quiz : Week3_Assignment1
- Feedback form for Week-3
- Assignment Solution

Week 4

Week3_Assignment1

The due date for submitting this assignment has passed. **Due on 2017-08-16, 23:59 IST**
As per our records you have not submitted this assignment.

1) Let $c \in \mathbb{Z}_{3750}$ such that $49^{1000} \equiv c \pmod{3750}$. Then $c =$

1 point

- 0
- 1
- 49
- 2

No, the answer is incorrect.

Score: 0

Accepted Answers:

1

2) Let $\phi(n)$ be the number of positive integers coprime to n and less than n . Then $\phi(437)$ is equal to

1 point

- 436
- 396
- 385
- 435

No, the answer is incorrect.

Score: 0

Accepted Answers:

396

3) Let $n = pq$, where $p = 67$ and $q = 127$. Suppose that there exist $a \in \mathbb{Z}_{\phi(n)}$ such that $ab \equiv 1 \pmod{\phi(n)}$, where $b = 41$. Then the value of a is

1 point

- 1219
- 1200
- 1218
- 1217

No, the answer is incorrect.

Score: 0

Accepted Answers:

1217

4) Consider an RSA cryptosystem with $n = pq$, where $p = 13$ and $q = 29$. Let the public key be $(n, 25)$. Then the encrypted value of 10 is

1 point

- 114
- 192

- 208
- 121

No, the answer is incorrect.

Score: 0

Accepted Answers:

114

5) Consider an RSA cryptosystem with $n = pq$, where $p = 13$ and $q = 29$. Let the public key be $(n, 25)$. Then the decrypted value of 10 is

- 192
- 304
- 194
- 403

No, the answer is incorrect.

Score: 0

Accepted Answers:

192

6) Let the Legendre symbol value of $(4 / 19)$ and $(5 / 19)$ be r and s respectively. Then

1 point

- $r = 1, s = 1$
- $r = -1, s = -1$
- $r = -1, s = 1$
- $r = 1, s = -1$

No, the answer is incorrect.

Score: 0

Accepted Answers:

$r = 1, s = 1$

7) Suppose p is an odd prime and a is an integer such that $a^{((p-1)/2)} \equiv -1 \pmod{p}$. Then

1 point

- a is a quadratic residue modulo p .
- No such a exists.
- a is a quadratic non-residue modulo p .
- a is coprime to p .

No, the answer is incorrect.

Score: 0

Accepted Answers:

a is a quadratic non-residue modulo p .

8) The Jacobi symbol value of $(145 / 135)$ is

1 point

- 2
- 0
- 1
- 1

No, the answer is incorrect.

Score: 0

Accepted Answers:

0

9) The Jacobi symbol value of $(149 / 255)$ is

1 point

- 0
- 1
- 2
- 1

No, the answer is incorrect.

Score: 0

Accepted Answers:

-1

Previous Page

End



© 2014 NPTEL - Privacy & Terms - Honor Code - FAQs -

A project of



In association with



Funded by



Powered by

