Assignment 7

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

Due on 2019-03-20, 23:59 IST.

1) In ElGamal Public-Key Cryptosystem suppose $G = Z_{11} \setminus \{0\}$ and let $\alpha = 2$ as a primitive element private key $a = 3$. Suppose random number $k = 4$ then the ciphertext corresponding to plaintext

A. (5,6)  
B. (7,8)  
C. (3,1)  
D. (9,2)

2) The solution for the system of congruences $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$, $x \equiv 2 \mod 7$ is

A. 24  
B. 20  
C. 23  
D. 25

3) All quadratic residues modulo 17 are ______.

A. 1,2,4,8,9,13,15,16  
B. 1,2,4,8,9,13,14,16  
C. 1,2,4,8,9,11,15,16  
D. 1,2,3,8,9,13,15,16
Let \( p \) be an odd prime. Then \( a \) is a quadratic residue modulo \( p \) if and only if \( \frac{a^{(p-1)/2}}{1} \) (mod \( p \)).

A. \( a^{(p-1)/2} \equiv 1 \)
B. \( a^{(p-1)/2} \equiv 1 \)
C. \( a^p \equiv 1 \)
D. \( a^{(p+1)/2} \equiv 1 \)

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

In Rabin Cryptosystem, let \( n = pq \) where \( p \) and \( q \) are primes and \( p, q \equiv 3 \) (mod 4). In this cryptosystem, encryption function \( e \) and decryption function \( d \) is defined by \( e(x) = ______ \) mod \( n \) and \( d(y) = ______ \) mod \( n \) respectively.

A. \( \sqrt{x}, y^2 \)
B. \( x^p, \sqrt{y} \)
C. \( x^2, \sqrt{y} \)
D. \( x^q, \sqrt{y} \)

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

Consider the Rabin Cryptosystem with \( n = 161 \). Then the ciphertext corresponding to the plaintext \( P = 24 \) is

A. \( 93 \)
B. \( 90 \)
C. \( 91 \)
D. \( 92 \)

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

Let \( p = 1117 \), then for any integer \( a \) Legendre symbol \( \left( \frac{a}{p} \right) = ______ \) (mod \( p \)).

A. \( a^{258} \)
B. \( a^{1116} \)
C. \( a^{1117} \)
D. \( a^{1111} \)

No, the answer is incorrect.
Score: 0
Accepted Answers: A
Let $p$ be an odd prime and $a$ be an integer. Then $\sum_{x=1}^{p-1} \left( \frac{a}{p} \right)$ is ______. Note: $\left( \frac{a}{p} \right)$ is Legendre symbol.

A. 1  
B. -1  
C. 0  
D. $a$

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

9) The Legendre symbol $\left( \frac{5}{21} \right)$ is ______.

A. 1  
B. -1  
C. 0  
D. 2

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

10) If $a \equiv b \mod p$ then $\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) +$ ______ $\mod p$, where $p$ is an odd prime. Note: $\left( \frac{a}{p} \right)$ is Legendre symbol.

A. 1  
B. 2  
C. 0  
D. $p - 1$

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