Week 11 Assignment

The due date for submitting this assignment has passed.

Due on 2021-04-07, 23:59 IST.

As per our records you have not submitted this assignment.

Groups, cyclic groups, subgroups, cosets, Lagrange's Theorem, Dlog and applications, PKC: ElGamal and RSA encryption schemes

1) 1. Consider the following statements and choose the right option : *1 point*

I. The set of non-zero integers forms a group under multiplication operation
II. The set of real numbers forms a group under multiplication operation
III. The set of rational numbers forms an abelian group under addition operation

- I and II are correct
- II and III are correct
- I, II and III are correct
- Only III is correct

No, the answer is incorrect.
Score: 0
Accepted Answers:
Only III is correct

2) Let G be a cyclic group with a generator g whose order is 42. Which of the following is(are) true about G? *1 point*

- Only the elements g^{14} and g^{28} are of order 3
- There exist no elements of order 5, 6 and 10
- There are exactly 6 elements order 7.
- None of the given options

No, the answer is incorrect.
Score: 0
Accepted Answers:
Only the elements g^{14} and g^{28} are of order 3
There are exactly 6 elements order 7.

3) The total number of subgroups of a group G, with |G| = 29, is *1 point*

- 0
- 1
- 2
- 29

No, the answer is incorrect.
Score: 0
Accepted Answers:
2

4) The value of $\varphi(221)$, Euler's totient function, is *1 point*

- 72
- 120
- 144
- 192

No, the answer is incorrect.
Score: 0
Accepted Answers:
192

5) Consider the following statements and choose the right option(s) : *1 point*

I. Hashing can be used as a mechanism to keep data encrypted and safe from adversaries

II. In secure cryptosystems, the encryption and decryption algorithms are publicly available

III. When data is encrypted using cryptographically secure algorithms and sent through the internet it is guaranteed that it is always received correctly at the other end

- Only I is correct
- Only II is correct
- Only III is correct
- I and III are correct

No, the answer is incorrect.
Score: 0
Accepted Answers:
Only II is correct

6) Let $(G,\circ)$ be a finite abelian group of order n with identity element e_G. Let $x = a_1 \circ a_2 \circ \ldots \circ a_n$ where $G = \{a_i\}_{i=1}^{n}$. What is the value of x^{2016}? *1 point*

- 2016
- n
- Depends on the elements of G
- e_G

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

7) Let p ≥2 be a prime. How many generators are there in Z_p'? *1 point*

- $\varphi(p)$
- $\varphi(p-1)$
- p - 2
- 1

No, the answer is incorrect.
Score: 0
Accepted Answers:
$\varphi(p-1)$

8) Let $(G,\circ)$ be a finite cyclic group with generator g where the discrete log problem is hard. Specifically, it is hard to compute g^{ab} given g^a and g^b as required by the Diffie-Hellman key exchange protocol i.e., $DH(g^a, g^b) = g^{ab}$ is hard to compute. Which of the following functions are also hard to compute over G? *1 point*

- $f_1(g^a, g^b) = g^{2(a+b)}$
- $f_2(g^a, g^b) = g^{a(b+1)}$
- $f_3(g^a, g^b) = g^{2ab}$
- $f_4(g^a, g^b) = g^{a+b}$

No, the answer is incorrect.
Score: 0
Accepted Answers:
$f_2(g^a, g^b) = g^{a(b+1)}$
$f_3(g^a, g^b) = g^{2ab}$

9) Choose the correct statement(s) from the following? *1 point*

- Set of odd integers under addition is a subgroup of set of integers under addition
- $(Z_{p-1}, \cdot)$ where p is prime has p-1 elements that are co-prime to p
- Sender and receiver do not need to exchange their respective secret values to communicate over the public channel using El Gamal encryption scheme
- None of the given options

No, the answer is incorrect.
Score: 0
Accepted Answers:
$(Z_{p-1}, \cdot)$ where p is prime has p-1 elements that are co-prime to p
Sender and receiver do not need to exchange their respective secret values to communicate over the public channel using El Gamal encryption scheme

10) Which of the following statement(s) are incorrect? *1 point*

- The security of RSA cryptosystem depends on how the prime numbers p and q are chosen
- RSA cryptosystem can be broken if the order of Z_N^* is known
- None of the given options

No, the answer is incorrect.
Score: 0
Accepted Answers:
None of the given options