Week 11 Assignment

Due date for submitting this assessment has passed.

As per our records you have not submitted this assessment.

Groups, cyclic groups, subgroups, cosets, Lagrange's Theorem, Direct and indirect problems, MHD, RSA encryption in tenses

1. Consider the following statements and choose the right options:
   a. The set of even numbers forms a group under multiplication operation.
   b. The set of all non-zero numbers forms a group under multiplication operation.
   c. The set of all integers forms a group under addition operation.
   d. 1 and 0 are inverses of each other.
   e. 1 and 0 are not inverses of each other.
   f. None of the above.

   Accepted Answer: Only D is correct.

2. Let (G, *) be a group with a generator g such that order is 2. Which of the following is true about G?
   a. Only the identity element e has order 2.
   b. There are no elements of order 3 or order 4.
   c. There are exactly 3 elements of order 7.
   d. None of the above.

   Accepted Answer: Only the identity element e has order 2.

3. The number of subgroups of a group G with |G| = 36 is
   a. 1
   b. 2
   c. 3
   d. 29

   Accepted Answer: 3

4. The value of $g^{2251}$, where $g$ is a generator of $Z_{2251}^*$, is
   a. 12
   b. 121
   c. 143
   d. 143

   Accepted Answer: 121

5. Consider the following statements and choose the right option(s):
   a. Hashing can be used as a mechanism to keep data encrypted and safe from unauthorized access.
   b. In secure cryptosystems, the encryption and decryption algorithms are publicly available.
   c. When data is encrypted using mathematical algorithms and sent through the Internet, it is guaranteed that it is always received correctly by the other side.

   Accepted Answer: Only C is correct.

6. Let $(G, .)$ be a finite abelian group of order $n$ with identity element e. Let $p = p_1 p_2 \ldots p_k$ be the prime factorization of $n$.
   a. Write $G$ as $Z_{p_1} \times Z_{p_2} \times \ldots \times Z_{p_k}$, what is the value of $n^{p}$?
   b. Depends on the elements of $G$
   c. No, the answer is incorrect.
   d. Accepted Answer: 1

7. Let $n$ be a prime. How many generators are there in $Z_n^*$?
   a. $\varphi(n)$
   b. $\varphi(n) - 1$
   c. 1
   d. No, the answer is incorrect.

   Accepted Answer: $\varphi(n) - 1$

8. Let $(G, \cdot)$ be a finite cyclic group with generator $g$, where the discrete log problem is hard. Specifically, it is hard to compute $g^x$, given $g^x$ and $g$ as required. Let the Diffie-Hellman key exchange protocol $\{k, (g^a)^b\}$ be hard to compute. Which of the following functions are also hard to compute over $\mathbb{Z}_n$?
   a. $g^{a} \cdot g^{b} = g^{a+b}$
   b. $g^{a \cdot b} = g^{ab}$
   c. $g^{a+b} = g^{a} \cdot g^{b}$
   d. No, the answer is incorrect.

   Accepted Answer: $g^{a \cdot b} = g^{ab}$

9. Choose the correct statement(s) from the following:
   a. Set of odd integers under addition is a subgroup of set of integers under addition
   b. $Z_3$ under addition has 3 elements that are co-prime to each other.
   c. Gender and race do not matter to exchange their respective secret values to communicate over the public channel using ElGamal encryption scheme.
   d. Some of the given options

   Accepted Answer: None of the given answers

10. Which of the following statements is incorrect?
    a. The security of RSA cryptosystem depends on how the prime numbers $p$ and $q$ are chosen.
    b. RSA cryptosystem can be broken if the order of $Z_n$ is known.
    c. None of the given statements
    d. No, the answer is incorrect.

   Accepted Answer: None of the given options