| Examination: Quiz 2  Duration: 30 minutes | Semester: Summer 2022  Full Marks: 20 |
| --- | --- |

CSE 447: Cryptography and Cryptanalysis

| **Name:** | **ID:** | **Section: 01** |
| --- | --- | --- |

| 1 | For the elements of the Galois field of (), Calculate, *A(x) \* B(x).* Irreducible polynomial is [CO2] | 4 |
| --- | --- | --- |
| 2 | Suppose a server sends P to one of its clients, as follows. [CO2]  = 1101, = 1001, = 0111, = 0101 and Initializing vector (IV) was 0000.  Along with the above values, the server also sends the MAC = 0111.  **Investigate** whether the value of P is modified or not. | 6 |
| 3 | Suppose you are given 2 Knapsacks as (5, 7, 17, 39, 75, 150, 301) [CO2]   1. For that superincreasing knapsack calculate the value of General Knapsack. Assume, you are given m=37 and n= 601. 2. You need to Encrypt 1101011 and **Illustrate** that you get the same value after Decrypting. Show the detailed procedure of inverse calculation. | 7 |
| 4 | “The attacker has access to the ciphertext and its corresponding plaintext”. [CO1]   1. **Identify** the type of cryptanalysis attack. 2. “This attack can be successful”, **Justify** your answer. | 3 |