**20CB401/MA05**

**Hall Ticket Number:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **II/IV B.Tech (Regular) DEGREE EXAMINATION** | | | |
| **August, 2022** | **CYBER SECURITY** | | |
| **Fourth Semester** | **Mathematical Foundations for Cyber Security** | | |
| **Time:** Three Hours | | **Maximum:** 70 Marks | |
| *Answer Question No.1 compulsorily.* | | | (1X14 = 14 Marks) |
| *Answer ONE question from each unit.* | | | (4X14=56 Marks) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | | Answer all questions. | | | (14X1=14 Marks) | |
|  | | a) | | Define Modulus | |  |
|  | | b) | | What is the difference between modular arithmetic and ordinary arithmetic? | |  |
|  | | c) | | What does it mean to say that b is a divisor of a? | |  |
|  | | d) | | What are the operations of modular arithmetic | |  |
|  | | e) | | Why? | |  |
|  | | f) | | Define a Group | |  |
|  | | g) | | What is Euler’s totient function? | |  |
|  | | h) | | Determine Φ(440) | |  |
|  | | i) | | Find all primitive roots of 25 | |  |
|  | | j) | | What is a perfect code? | |  |
|  | | k) | | Given C={00000, 01010, 10101,11111}, find the minimum distance of the code C | |  |
|  | | l) | | What is Symmetric Key Cryptography? | |  |
|  | | m) | | Define crypt analysis. | |  |
|  | | n) | | What is cipher text? | |  |
| **UNIT I** | | | | | | |
| 2. | a) | | Solve GCD(1970,1066) using Euclid’s algorithm | | | 7M |
|  | b) | | Find all additive inverse Pairs and Multiplicative inverses in Z10 | | | 7M |
| **(OR)** | | | | | | |
| 3. | a) | | Prove that the set G = {0, 1, 2, 3, 4} is an abelian group under addition modulo 5. | | | 7M |
|  | b) | | For the finite field with defining polynomial f(x)= , calculate the following ) X | | | 7M |
| **UNIT II** | | | | | | |
| 4. | a) | | State Fermat’s Theorem and solve 72019 mod 13 | | | 7M |
|  | b) | | Use the Miller-Rabin Primality Test to test whether n = 157 is a prime. Choose the random value a = 8. | | | 7M |
| **(OR)** | | | | | | |
| 5. | a) | | Solve the simultaneous congruence  X ≡ 6 mod 11, X ≡ 13 mod 16, X ≡ 9 mod21, X ≡ 19 mod 25 Using Chinese Remainder theorem | | | 7M |
|  | b) | | State Euler’s theorem. Solve 499 mod 35 using Euler’s theorem. | | | 7M |
| **UNIT III** | | | | | | |
| 6. | a) | | Let G7 =  Show that G7 generates an optimal linear code, that is, show that the largest minimum weight among all binary linear [7, 2] codes is 4. | | | 7M |
|  | b) | | Consider a (5,1) linear block code defined by the generator matrix G = [1 1 1 1 1]   1. Determine the number of information and parity check bits for each code word. 2. Write down the parity check equations. 3. C) List all code vectors and find the minimum Hamming distance of the code. | | | 7M |
| **(OR)** | | | | | | |
| 7. | a) | | If then find a linear block code generated by . Also find the minimum distance of this code. | | | 7M |
|  | b) | | Let be a binary perfect code of length with minimum distance. Then show that or | | | 7M |
| **UNIT IV** | | | | | | |
| 8. | a) | | Apply Vigenere cipher; encrypt the word “Explanation” using the key leg. | | | 7M |
|  | b) | | Apply play fair cipher method to encrypt the word “Semester result” with keyword  “Examination”. | | | 7M |
| **(OR)** | | | | | | |
| 9. | a) | | Develop Cipher Text of the given text “Andhra Pradesh” using rail fence technique. | | | 7M |
|  | b) | | Explain Transposition Technique with an example | | | 7M |

