**20CB401**

**Hall Ticket Number:**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **II/IV B.Tech (Regular\Supplementary) DEGREE EXAMINATION** | | | |
| **July/August, 2023** | **Cyber Security** | | |
| **Fourth Semester** | **Mathematical Foundations for Cyber Security** | | |
| **Time:** Three Hours | | **Maximum:** 70 Marks | |
| ***Answer question 1 compulsory.*** | | | **(14X1 = 14Marks)** |
| ***Answer one question from each unit.*** | | | **(4X14=56 Marks)** |
|  | | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | CO | BL | M |
| 1 | a) | Define Modulus | CO1 | L2 | 1 |
|  | b) | Determine whether the set {-1, 0, 1} forms a subgroup of the group of integers under addition. | CO1 | L2 | 1 |
|  | c) | Use the division algorithm to express 187 as the product of its quotient and divisor when divided by 13. | CO1 | L2 | 1 |
|  | d) | State Fermat's theorem. | CO2 | L1 | 1 |
|  | e) | Find the remainder when 717 is divided by 10 using Euler's theorem. | CO2 | L1 | 1 |
|  | f) | Compute the discrete logarithm of 8 with base 3 modulo 17. | CO2 | L3 | 1 |
|  | g) | Find all primitive roots of 25 | CO2 | L2 | 1 |
|  | h) | What is the relation between d\* and w\* in a linear code | CO2 | L1 | 1 |
|  | i) | Write the systematic form of generator matrix | CO3 | L2 | 1 |
|  | j) | What is perfect code | CO3 | L1 | 1 |
|  | k) | Define symmetric-key cryptography | CO3 | L2 | 1 |
|  | l) | Encrypt the message "CRYPTOGRAPHY" using a columnar transposition cipher with the keyword "SECURITY." | CO4 | L2 | 1 |
|  | m) | List the advantages of Monoalphabetic Substitution Ciphers. | CO4 | L1 | 1 |
|  | n) | What are the two basic functions used in encryption | CO4 | L2 | 1 |
| **Unit-I** | | | | | |
| 2 | a) | Solve GCD(1759, 550)=1759 x+ 550 y by extended Euclidean algorithm | CO1 | L2 | 7M |
|  | b) | Find all additive inverses and multiplicative inverses in Z10 | CO1 | L2 | 7M |
|  |  | **(OR)** |  |  |  |
| 3 | a) | Compute the division (x5 + x3 + 1) ÷ (x2 + x) in GF(2)[x] and express the quotient and remainder. | CO1 | L3 | 7M |
|  | b) | Prove that Z11 is a field over modulus arithmetic modulo 11 | CO1 | L2 | 7M |
| **Unit-II** | | | | | |
| 4 | a) | Prove the primality of the number 561 using the Miller-Rabin algorithm. | CO2 | L5 | 7M |
|  | b) | Solve the congruence equation 3^x ≡ 5 (mod 17) using logarithms for modular arithmetic. | CO2 | L3 | 7M |
| **(OR)** | | | | | |
| 5 | a) | State and Prove Fermat’s Little Theorem. | CO2 | L5 | 7M |
|  | b) | Apply the Pollard's rho algorithm to calculate the discrete logarithm of 3 with respect to base 5 modulo 19. | CO2 | L3 | 7M |
| **Unit-III** | | | | | |
| 6 | a) | For each of the following sets S, write list the <S>,   1. S{0101, 1010, 1100} (ii) S={1000, 0100, 0010, 0001} (iii) S={ 11000, 01111, 11110, 01010} | CO3 | L2 | 7M |
|  | b) | Explain the concept of syndrome decoding for linear block codes. Derive the relationship between the syndrome and the error pattern for a received codeword. | CO3 | L2 | 7M |
| **P.T.O**  **20CB401**  **(OR)** | | | | | |
| 7 |  | For a (5,3) code over GF(4), the generator matrix is given by   1. Find the parity check matrix 2. How many errors can this code detect 3. How many errors can this correct 4. How many erasures can this code correct 5. Is this a perfect code | CO3 | L2 | 14M |
| **Unit-IV** | | | | | |
| 8 | a) | Explain how the Caesar cipher works and provide an example of encrypting the message "HELLO" with a key of 3. Show the complete encryption process. | CO4 | L4 | 7M |
|  | b) | Explain how the Hill cipher works and demonstrate the encryption of the message "HELLO" using a 2x2 key matrix. | CO4 | L4 | 7M |
| **(OR)** | | | | | |
| 9 | a) | Explain how the Rail Fence cipher works and demonstrate the encryption and decryption process for the message "HELLO" using a rail count of 3. | CO4 | L5 | 7M |
|  | b) | Encrypt the plaintext "ENCRYPTION" using the keys "KEY1" and "KEY2" using Double Transposition Cipher. | CO4 | L4 | 7M |

