Hall Ticket No | | | | | | | | | | | Question Paper Code: ACCC01

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal-500043, Hyderabad

B.Tech III SEMESTER END EXAMINATIONS (REGULAR/ SUPPLEMENTARY) - FEBRUARY 2024

Regulation: UG20

(MATHEMATICAL FOUNDATION FOR CYBER SECURITY)

Time: 3 Hours **CSE(CYBER SECURITY)** **Max Marks: 70**

Answer ALL questions in Module I and II
Answer ONE out of two questions in Modules III, IV and V
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

MODULE – I

1. (a) Explore the step-by-step process of the Euclidean algorithm, which involves iteratively applying the division remainder operation until reaching a remainder of zero.

[BL: Understand| CO: 1|Marks: 7]

(b) Solve the simultaneous congruences x= 6(mod11), x = 13(mod16), x = 9(mod21), x = 19(mod25).

[BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) What are subrings, ideals, and quotient rings in abstract algebra, and how do these concepts contribute to the study of ring theory and algebraic structures?

[BL: Understand| CO: 2|Marks: 7]

(b) Let R be a group of all real numbers under addition and R+ be a group of all positive real numbers under multiplication. Show that the mapping f : R $\rightarrow$ R+ defined by f(x) = 2^x for all x R is an isomorphism. [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) Write about discrete-random processes. How do they differ from continuous-random processes? Describe the key characteristics and components of discrete-random processes.

[BL: Understand| CO: 3|Marks: 7]

(b) Outline about conditional probability in terms of the probability of event B given event A, denoted as P(B|A), and discuss how it can be calculated using the formula P(B|A) = P(A $\cap$ B)/P(A), where P(A $\cap$ B) represents the probability of both events A and B occurring.

[BL: Understand| CO: 3|Marks: 7]

4. (a) Describe the essential components of Markov chains, including state spaces, transition probabilities, and the memoryless property with transition diagram.

[BL: Understand| CO: 4|Marks: 7]

(b) The record of weights of the male population follows the normal distribution. Its mean and standard deviations are 70 kg and 15 kg respectively. If a researcher considers the records of 50 males, then what would be the mean and standard deviation of the chosen sample? Using central limit theorem. [BL: Apply| CO: 4|Marks: 7]

MODULE – IV

5. (a) Explore the principles behind next-bit predictors, which aim to forecast the value of the next bit in a data stream based on patterns and correlations observed in previous bits.

   [BL: Understand| CO: 5|Marks: 7]

   (b) Let C be a binary (5,3) code with generator matrix, G= 10110 11010 01001

   i) Reduce G to standard form.

   ii) Find a parity-check matrix for C.

   iii) Write out the elements of the dual code C [BL: Apply| CO: 5|Marks: 7].

6. (a) Compare and contrast the error detection and correction capabilities of Hamming codes, Hadamard codes, and Goppa codes in the context of forward error correction.

   [BL: Understand| CO: 5|Marks: 7]

   (b) A binary symmetric channel has probability p = 0.05 of incorrect transmission. If the code word c = 011 011 101 is transmitted. What is the probability that

   i) We receive r = 011 111 101

   ii) We receive r = 111 011 100

   iii) A single error occurs

   iv) A double error occurs

   v) A triple error occurs [BL: Apply| CO: 5|Marks: 7]

MODULE – V

7. (a) Write the importance of pseudorandom number generation in various computational tasks, including simulations, cryptography, and randomized algorithms. Explain the different types used to generate pseudorandom numbers. [BL: Understand| CO: 6|Marks: 7]

   (b) Describe in detail about Blum blum shub bit generator. Find the first 8 bits for Blum blum shub bit generator when seed = 101355 and n = 192649. [BL: Understand| CO: 6|Marks: 7]

8. (a) Discuss in detail about random and pseudorandom generators with necessary diagrams and differentiate them. [BL: Understand| CO: 6|Marks: 7]

   (b) Show that A PRG G passes all polynomial time statistical tests if and only if it passes all polynomial time next-bit tests. [BL: Apply| CO: 6|Marks: 7]

– ○ ○ ◯ ○ ○ –