Hall Ticket No | | | | | | | | | | | Course Code: ACCCO1

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal, Hyderabad - 500 043

B.Tech III SEMESTER END EXAMINATIONS (REGULAR / SUPPLEMENTARY) - FEBRUARY 2023
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) Show that no positive integer of the form $4n(8m + 7)$ can be represented as the sum of three squares. [BL: Apply| CO: 1|Marks: 7]

   (b) Find the greatest common divisor g of the numbers 42823 and 6409 and then find the integers of x and y to satisfy $42823x + 6409y = g$ [BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) Discuss cyclic group and latice. Prove that every cyclic group is an abelian . [BL: Apply| CO: 2|Marks: 7]

   (b) Show that the set G = { 1, -1 , i , -i } i.e., four roots of unity form a finite abelian group with respect to multiplication. [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) Find the unique fixed probability vector for the regular stochastic matrix $\begin{bmatrix} 0 & 1 & 0 \\ 1/6 & 1/2 & 1/3 \\ 0 & 2/3 & 1/3 \end{bmatrix}$ [BL: Apply| CO: 3|Marks: 7]

   (b) In a certain college 4% of boys and 1% of girls are taller than 1.8m. Also 60% of the students are girls. If a student is selected at random and found taller than 1.8m, what is the probability that the student is a girl? [BL: Apply| CO: 3|Marks: 7]

4. (a) Suppose that a random sample of size 100 is taken from the inner diameters of certain lengths of pipes. If the mean and standard deviation of such measurements are 34.1 and 1.5 inches respectively, using central limit theorem find the probability that the sample mean will be between 34 and 34.3 [BL: Apply| CO: 4|Marks: 7]

   (b) A single fair dice is rolled.

   i) Let A=3 and B=1,3,5. Are A and B independent.

   ii) Find the probability that the number rolled is odd, given that it is a five.

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

MODULE – IV

5. (a) In the 5 repeat code of V(5,4) (codeword's: 00000, 11111, 22222, and 33333) What is the minimum distance. [BL: Apply| CO: 5|Marks: 7]

   (b) Let C be a binary (5, 3) code with generator matrix, G= $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

   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) Write Hadamard matrix of order n with an example. Explain any two properties of Hadamard matrix. [BL: Understand| CO: 5|Marks: 7]

   (b) Suppose the parity-check matrix of a binary linear code is $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

   Decode each of the following received words: 111000, 101001 and 001101.

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

MODULE – V

7. (a) Justify that the quadratic residuosity problem and solver is suitable for security of the BBS generator. [BL: Understand| CO: 6|Marks: 7]

   (b) Let n=p.q be the product of two blum primes. Show that
   $\forall x \in Z_n(+1)x \in R_n \Leftrightarrow parity(x) = parity(\sqrt{x^2}(modn))$ [BL: Apply| CO: 6|Marks: 7]

8. (a) Describe in detail about security of the BBS generator with an example of LCG generator. [BL: Apply| CO: 6|Marks: 7]

   (b) Show that there exist one way permutations f with hard core bit B, then there exist CS PRG $G : 0, 1n \rightarrow 0, 1m(n)$ for any polynomial m. [BL: Apply| CO: 6|Marks: 7]

– ∘ ∘ ◯ ∘ ∘ –