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

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

(Dundigal-500043, Hyderabad)

B.Tech III SEMESTER END EXAMINATIONS (REGULAR) - FEBRUARY 2022

Regulation:UG-20

MATHEMATICAL FOUNDATION FOR CYBER SECURITY

Time: 3 Hours **(CS)** **Max Marks: 70**

Answer ALL questions in Module I and II

Answer ONE out of two questions in Modules III, IV and V

NOTE: Provision is given to answer TWO questions from among one of the Modules III / IV / V

All Questions Carry Equal Marks

All parts of the question must be answered in one place only

MODULE – I

1. (a) Use the Euclidean algorithm to find the GCD(1819,3587) **[7M]**

   (b) Find the remainder when the sum $1! + 2! + 3! + ... + 1000!$ is divided by 4 and by 5. **[7M]**

MODULE – II

2. (a) Show that if $\{U_n\}$ is the set of n^{th} roots of unity, $\{U_n, x\}$ is a cyclic group. Is it abelian? **[7M]**

   (b) If R and C are additive groups of real and complex numbers respectively and if the mapping $f : C \to R$ is defined by $f(x + iy) = x$, show that f is a homomorphism. Find also the kernel of f. **[7M]**

MODULE – III

3. (a) Use Bayes'theorem to find $p(W = j|M = k)$ where i and j and k are distinct values. **[7M]**

   (b) There are 250 dogs at a dog show who weigh an average of 12 pounds, with a standard deviation of 8 pounds. If 4 dogs are chosen at random, what is the probability they have an average weight of greater than 8 pounds and less than 25 pounds using central limit theorem. **[7M]**

4. (a) A continuous random variable X has a p.d.f.
   $f(x) = 3x^2, 0 \leq x \leq 1$ Find a and b such that
   i) $P(X \leq a) = P(X > a)$
   ii) $P(X > b) = 0.05$.
   [7M]

   (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? Use central limit theorem. **[7M]**

MODULE – IV

5. (a) 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

[7M]

(b) Find the code words generated by the parity check matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ when the encoding function is $e : B^3 \rightarrow B^6$. **[7M]**.

6. (a) Write about Hadamard matrix. Construct a 4x4 Hadamard matrix. **[7M]**

(b) Let C1 be linear binary [6,3,3] code with generator matrix $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ and parity check matrix $\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ Find the syndromes and coset leaders. **[7M]**

MODULE – V

7. (a) Explain quadratic residues and find the quadratic residues and non-quadratic of Z_{23}^* **[7M]**

(b) Let p be an odd prime and let $a \epsilon Z_p^*$ then show that $(\frac{a}{p}) = a^{\frac{p-1}{2}}$ (mod p) **[7M]**

8. (a) Let $G : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a PRG. For any polynomial l, $G^{'} : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$, $G^{'}(s) = b_1, ...b_{l(n)}$ where $X_0 \leftarrow s \Rightarrow X_{i+1}||b_{i+1} \leftarrow G(X_i)$ then G is a PRG. Let n be an integer and let a and b be integers then

[7M]

(b) Let n be an integer and let a and b be integers then show that $\frac{ab}{n} = (\frac{a}{n})(\frac{b}{n})$ **[7M]**

– ∘ ∘ ◯ ∘ ∘ –