Mahindra University
University
Global Thinkers, Engaged Leaders.

Mahindra University Hyderabad
École Centrale School of Engineering
Minor - 2
Program: B. Tech Branch: CSE/ARI/CAM/CAB/ECM/ECE Year: I Semester:2
Subject:- Discrete Mathematical Structures (CS 1202)

Date: 01/05/2023 **Start Time: 10:00 AM**
Time Duration: 1 h 30 m **Max. Marks: 100**

Instructions:

- Answer all the questions.
- All the sub-questions belonging to a big question should be answered together.
- Total marks are set to 100 only for convnience. There is nothing to worry. Answer what you can, happily.

Q1: RSA encryption

Marks: $5 \times 4 = 20$M

A quick recap of how the RSA algorithm works:

Bob's side	Alices's side
1) Setting up • Generates two prime numbers p and q such the product $n = p \times q$ is large enough. • Generates a public-key (n, e), and displays it for the public. (Remember how?) • Generates a private-key (n, d), and keeps it a secret. (Remember how?) **3) Reception** • Receives the ecrypted message M_e. • Finds the original message by performing the computation $remainder(M_e^d, n)$.	**2) Transmission** • Alice decides on the message M to be trasnmitted to Bob. • Alice looks up for Bob's public-key (n, e) and encrypts M and converts it to M_e. (Remember how?) • Broadcasts M_e with absolute confidence that only Bob can decrypt this message. (Remember why?)

Answer the following questions:

1. How large should $n = p \times q$ be in order to be large enough?
2. Suppose the two primes that Bob generates are $p = 11$ and $q = 3$. What is the totient m?
3. Supposing $e = 7$, what is the value of d, the multiplicative inverse of $e \pmod{n}$?
4. Suppose Alice's secret message is $M = 17$. What is the encrypted message (M_e) that Alice broadcasts?
5. Suppose Bob receives $M_e = 3404825447$. What is the corresponding decrypted message M?

Q2: Summations

Marks: $4 \times 5 = 20$M

Consider the following summation

$$S(n) = 1 - 2^2 + 3^2 - 4^2 + 5^2 + \ldots (-1)^{n-1} n^2$$

Answer the following questions

1. Compute the value of $S(1)$.
2. Compute the value of $S(10)$.
3. Find the closed form expression for any general n.
4. Compute the value of $S(201)$.

Q3: GCD

Marks: $2 \times 10 = 20$M

1. Compute the value of $gcd(1147, 899)$.
2. Compute c_1 and c_2 where $gcd(7, 20) = c_1.7 + c_2.20$.

Q4: Fundamental Theorem of arithmetic

Marks: $2 \times 10 = 20$M

1. Prime factorize 4087.
2. Prime factorize 43751.

Q5: Modular Artithmetic

Marks: $2 \times 10 = 20$M

1. Find the remainder when 3^{123} divided by 7.
2. Solve the following congruence relation for x

$$84x - 38 \equiv 79 (mod 15)$$
