Mahindra University
University

Mahindra University Hyderabad
École Centrale School of Engineering
Minor-I

Program: B. Tech. Branch: CM Year: II Semester: II
Subject: Number Theory & Cryptography (MA 2209)

Date: 28/02/2024 **Start Time: 02.00 PM**
Time Duration: 90 minutes **Max. Marks: 30**

Instructions:

1. There are 4 questions, all of which are compulsory.
2. Justify your answer wherever required.

---

1. (a) Find $100^{-1}(\mod 143)$. [4]
   (b) Using Fast Powering Algorithm compute $3^{253}(\mod 1000)$. [4]

---

2. Suppose that $k = (6, 10)$ is a key in an Affine Cipher over $\mathbf{Z}_{43}$. Decrypt the ciphertext 31. [8]

---

3. Bob's RSA public key cryptosystem has modulus $n = 221$ and encryption exponent $b = 5$. Alice sends Bob the ciphertext $c = 100$. Unfortunately, Bob has chosen too small a modulus. Help Eve in decrypting Alice's message. [10]

---

4. Let a, b, c be integers such that $gcd(a, b, c) = 1$, i.e., the largest integer dividing all of a, b, c is 1. Using extended euclidean algorithm (The Theorem) show that the equation $au + bv + cw = 1$ has a solution in integers u, v, w. [4]
