Mahindra University
Global Thinkers. Engaged Leaders

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: 6/03/2023 **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) Is 2 a primitive root mod 11? Justify your answer. [4]
   (b) Compute $11^{183} \pmod{100}$. [4]

---

2. Suppose that $k = (8, 11)$ is a key in an Affine Cipher over $\mathbb{Z}_{37}$. Decrypt the ciphertext 31. [6]

---

3. Bob's RSA public key has modulus $n = 187$ and encryption exponent $b = 53$. Alice sends Bob the ciphertext $c = 90$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. [8]

---

4. Solve the following simultaneous systems of congruences using Chinese Remainder Theorem.

   $x \equiv 2 \pmod{5}$, $x \equiv 6 \pmod{11}$, and $x \equiv 9 \pmod{13}$. [8]