Mahindra
University
Global Thinkers. Engaged Leaders.

Mahindra University Hyderabad
École Centrale School of Engineering
Minor II

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

Date: 16/04/2024 **Start Time: 02.00 PM**
Time Duration: 1.5 Hours **Max. Marks: 30**

Instructions:

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

1. (a) Show that 3 is a primitive root modulo 89 (without computing all the powers of 3 modulo 89). [4]

   (b) Using Shank's algorithm solve the following discrete logarithm problem: [7]

$$3^x \equiv 2 \mod 89.$$

2. Compute all the square roots of 1 modulo 77. [5]

3. (a) Let p be an odd prime and let g be a primitive root modulo p. Prove that a has a square root modulo p if and only if its discrete logarithm $\log_g(a)$ modulo p is even. [2]

   (b) Let p be a prime satisfying $p \equiv 3 \mod 4$. Let a be an integer such that a has a square root modulo p. Use (a) to prove that $b \equiv a^{(p+1)/4}(\mod p)$ is a square root of a. [3]

4. (a) Evaluate the Jacobi symbol $\left(\frac{7411}{9283}\right)$. [4]

   (b) Is 3 a Miller-Rabbin Witness for 45? [5]