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: 29/04/2023 **Start Time: 02.00 PM**
Time Duration: 1.5 Hours **Max. Marks: 30**

Instructions:

1. There are 5 questions, all of which are compulsory.
2. Justify your answer wherever required.

---

1. Alice and Bob agree to use the prime $p = 31$ and the base (primitive root) $g = 3$ for communications using the ElGamal public key cryptosystem. Bob chooses $a = 11$ as his private key.
   (a) What is the value of his public key A? **[2]**
   (b) Bob encrypts the message $m = 29$ using the ephemeral key $k = 7$. What is the ciphertext (c_1, c_2) that Bob sends to Alice? **[2]**
   (c) How does Alice get back m from the ciphertext (c_1, c_2)? **[2]**
   (d) What is the ciphertext if Bob uses the ephemeral key $k = 3$? Verify that Alice gets back the same message m if she uses this ciphertext. **[3]**

---

2. (a) Evaluate the Jacobi symbol $\left(\frac{610}{987}\right)$. **[2]**
   (b) Is 9 a Miller-Rabbin Witness for 41? **[4]**

---

3. Compute all the square roots of 1 modulo 187. **[5]**

---

4. (a) Let p be an odd prime and g be a primitive root modulo p. Prove that g^m is a quadratic residue modulo p if and only if m is even. **[3.5]**

(b) Deduce that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. [1.5]

---

5. Assuming the case $k = 2$ prove the following:

Let $a_1, a_2, ..., a_k$ be integers and $gcd(a_1, a_2, ..., a_k)$ denote the largest positive integer dividing all of $a_1, ..., a_k$. Then there exists integers $u_1, u_2, \ldots u_k$ such that

$$a_1u_1 + a_2u_2 + \ldots + a_ku_k = gcd(a_1, a_2, ..., a_k).$$

[5]