Mahindra University
University
Global Thinkers. Engaged Leaders.

**Mahindra University Hyderabad**
**École Centrale School of Engineering**
**Spring Semester Regular Examinations,**
**May-2024**

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

**Date: 28/05/2024** **Start Time: 10:00 AM**
**Time Duration: 3 Hours** **Max. Marks: 100**

---

**Instructions:**

1. There are 7 questions. All of which are compulsory. The credit for each question is mentioned at the end of the question.
2. Justify your answer wherever required.
3. All notations are standard and same as used in the lectures.

1. (a) Compute $2^{102} \pmod{77}$. **[4]**
   (b) Compute $(1,10) - (3,9)$ in the elliptic curve $x^3 + 5x + 6$ over $\mathbb{Z}_{11}$. **[5]**
   (c) Evaluate the Jacobi symbol $\left(\frac{549}{2457}\right)$. **[4]**
   (d) Using Euclidean Algorithm compute gcd(2154, 978) **[3]**
   (e) Find a witness for compositeness of 10. **[4]**

---

2. For $n = pq$, where $p$ and $q$ are distinct odd primes, define

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

Suppose that we modify the RSA cryptosystem by requiring that $ab \equiv 1 \pmod{\lambda(n)}$ where $a$ and $b$ are decryption and encryption exponents respectively.

(a) Prove that encryption and decryption are still inverse operations in this modified cryptosystem. **[10]**
(b) If $p = 53, q = 71$, and $b = 5$, decrypt the ciphertext 3 in this modified cryptosystem. **[5]**

---

3. Alice and Bob agree to use the prime $p = 83$ and the primitive root $g = 5$ for communications using the ElGamal public key cryptosystem. Bob chooses $a = 9$ as his private key.

   (a) What is the value of his public key $A$? [4]

   (b) Alice encrypts the message $m = 14$ using the ephemeral key $k = 6$. What is the ciphertext $(c_1, c_2)$ that Alice sends to Bob? [5]

   (c) How does Bob get back the message $m$ from the ciphertext $(c_1, c_2)$? [5]

---

4. Show that in an RSA cryptosystem, the modulus $n$ can be factored by computing Euler's Totient function, denoted as $\phi(n)$. [8]

---

5. Find an elliptic curve $E$ and a subgroup $H$ of $E$ such that $H$ is not cyclic. [8]

---

6. (a) Suppose Allice is using ElGamal Signature scheme with $p = 43$, primitve root $\alpha = 3$ and private key $a = 4$.

      (i) If Alice uses the secret random number $k = 5$ to sign the message $x = 10$. Compute her signature. [6]

      (ii) Suppose Bob receives the message $x = 7$ with signature $(\gamma, \delta) = (5, 23)$. Help him to verify the signature. [7]

   (b) Suppose Allice is using ElGamal Signature scheme with $p = 23$ and primitive root $\alpha = 5$. She sends Bob the message $x = 11$ with signature $(\gamma, \delta) = (17, 8)$. Unfortunately she has chosen too small a modulus. Help Oscar find the private key $a$. [7]

---

7. Let $E$ be the elliptic curve $y^2 = x^3 + 5x + 6$ over $\mathbb{Z}_{11}$.

   (a) Determine all the points in $E$. [6]

   (b) Show that $E$ is cyclic. [4]

   (c) Find all the elements of order 3. [5]

---