Mahindra University Hyderabad
École Centrale School of Engineering
End Semester Regular Examinations,
2025

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

Date: 30/05/2025 **Start Time: 10:00 AM**
Time Duration: 3 Hours **Max. Marks: 100**

Instructions:

1. There are 7 questions. All of which are compulsory. The marks allocated for each question are indicated at the end of the question.
2. Justify your answer wherever required.
3. Standard notations, consistent with those used in the lectures, are followed throughout.

1. (a) Compute $(2,6)-(6,0)$ in the elliptic curve x^3+2x+3 over $\mathbb{Z}_7$. [4]
   (b) Compute $3^{124} \pmod{93}$. [4]
   (c) Find a witness for compositeness of 6. [4]
   (d) Using the definition evaluate the Jacobi symbol $\left(\frac{347}{4725}\right)$. [4]
   (e) Evaluate the discrete logarithm $\log_2(11)$ for the prime 19. [4]

---

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

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

Suppose that we modify the RSA cryptosystem by requiring that $de \equiv 1 \mod \chi(n)$ where d and e are decryption and encryption exponents respectively. Prove that encryption and decryption are still inverse operations in this modified cryptosystem. [10]

---

3. Discuss the Pollard's $p-1$ factorization algorithm. [10]

OR

Discuss the vulnerability in the RSA cryptosystem known as the Common Modulus Protocol failure. (Recall that this occurs when Alice sends the same message to both Bob and Charlie, who are using RSA with the same modulus but different public exponents b_1 and b_2, such that $\gcd(b_1, b_2) = 1$.) **[10]**

---

4. (a) Show that 3 is a primitive root modulo 89. **[5]**

   (b) Using Shank's Algorithm solve the DLP $3^x \equiv 34 \mod 89$. **[10]**

---

5. Let E be the elliptic curve $y^2 = x^3 + 3x + 2$ over $\mathbb{Z}_7$.

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

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

   (c) Let $P = (0, 3), Q = (2, 3)$. Given that $P, Q \in E$, find $2P$. Does there exists a positive integer n such that $nQ = P$? If it exists, find such an n. **[5]**

---

6. (a) Suppose Allice is using ElGamal Signature scheme with $p = 53$ primitve root $\alpha = 2$ and private key $a = 5$ and $\beta = \alpha^a \mod p = 32$.

      (i) If Alice uses the secret random number $k = 3$ to sign the message $x = 21$. Compute her signature. **[6]**

      (ii) Suppose Bob receives the message $x = 9$ with signature $(\gamma, \delta) = (8, 7)$. How does he verify the signature? **[6]**

   (b) Suppose Allice is using ElGamal Signature scheme with $p = 29$ and primitive root $\alpha = 2$. She sends Bob the message $x = 9$ with signature $(\gamma, \delta) = (19, 12)$. Unfortunately she has chosen too small a modulus. Help Oscar find the private key a. **[6]**

---

7. Let E be the elliptic curve $y^2 = x^3 + 2x + 7$ defined over $\mathbb{Z}_{31}$. Given that the order of E is 39 and $P = (2, 9)$ is an element of order 39 in E. The *simplified ECIES* has $\mathbb{Z}_{31}^*$ as its plaintext space. Suppose the private key is $m = 8$. Decrypt the ciphertext $(y_1, y_2) = ((18, 1), 21)$. **[12]**

OR

Let E be an elliptic curve given by $y^2 = x^3 + ax + b \mod p$, where $p > 3$ is a prime. Prove that if $P = (x_1, y_1) \in E$ has order 3, then

$$3x_1^4 + 6ax_1^2 + 12x_1b - a^2 \equiv 0 \mod p.$$

Conclude that there are at most 8 points of order 3 on the elliptic curve E. **[12]**
