Mahindra University Hyderabad
École Centrale School of Engineering
Spring Semester Regular Examinations,
June-2023

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

Date: 06/06/2023 **Start Time: 10:00 AM**
Time Duration: 3 Hours **Max. Marks: 100**

Instructions:

1. There are 6 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 $-7503 \pmod{81.}$ [3]
   (b) Compute $(3,5)+(3,5)$ in the elliptic curve x^3+x+6 over $\mathbb{Z}_{11}$. [5]
   (c) Evaluate the Jacobi symbol $\left(\frac{4317}{7563}\right)$. [4]
   (d) Evaluate the discrete logarithm $\log_2(11)$ for the prime 19. [4]
   (e) Find all primitive roots modulo 7. [4]

---

2. Let E be the elliptic curve $y^2 = x^3+x+1$ over $\mathbb{Z}_5$.
   (a) Determine all the points in E. [7]
   (b) Show that E is cyclic. [7]
   (c) Let $P=(0,1), Q=(4,2)$. 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. [6]

---

3. a. Suppose that p is an odd prime and $\alpha \in \mathbb{Z}_p^*$. Show that α is a primitive element modulo p if and only if $\alpha^{\frac{p-1}{q}} \neq 1 \mod p$ for all primes q such that q divides $p-1$. [8]

$x_3 = \lambda^2 - x_1 - x_2$
$y_3 = \lambda(x_1 - x_3) - y_1$

b. Using the above statement prove that 2 is a primitive element modulo 101. [7]

---

4. 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 $ab \equiv 1(\mod \lambda(n))$ 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 $p = 43, q = 67$, and $b = 5$, compute the decryption exponent a in this modified cryptosystem. [5]

---

5. a. Suppose Allice is using ElGamal Signature scheme with $p = 47$, primitve root $\alpha = 5$ and private key $a = 8$.

(i) If Alice uses the secret random number $k = 9$ to sign the message $x = 38$. Compute her signature for her. [6]

(ii) Suppose Bob receives the message $x = 45$ with signature $(\gamma, \delta) = (11, 7)$. Help him to verify the signature. [7]

b. Suppose Allice is using ElGamal Signature scheme with $p = 23$. She sends Bob the message $x = 16$ with signature $(\gamma, \delta) = (9, 0)$. Help Oscar to find the private key a. [7]

---

6. Given that 5 is a primitive root of $\mathbb{Z}_{43}$, solve the DLP $5^x \equiv 13 \ (\mod 43)$ using Shank's Algorithm. [10]