Name_____ **Entry No:**_____

Indian Institute of Technology Delhi
Major Examination
MTL-730 (Cryptography)

Time: 2 Hours (+30 minutes uploading time) Max. Marks: 50

Attempt all questions. All notations are standard. All parts of a question must be answered at one place. Exhibit clearly all the steps. Calculator is allowed. No query will be entertained. ***In each question write all the steps/calculations clearly. No marks will be given for direct answers. Upload your answer sheet before 11:30 AM, only on Gradescope.***

1. (a) Using the fact $99^2 \equiv 25^2 \pmod{1147}$. Find the factors of 1147. [1 marks]
   (b) Prove or disprove $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$ is divisible by 4. [2 marks]
   (c) Show that $p > 3$ is prime then $p^2 \equiv 1 \pmod{24}$. [2 marks]
   (d) Find all solutions of congruence $3x^2 + 5x + 2 \equiv 0 \pmod{2537}$ [4 marks]

2. If $n = 493$, find the smallest factor base $\mathcal{B}$ such that squares of 23, 27, 29, 31, 32 are $\mathcal{B}$-numbers and then factor n. [2 marks]

3. Let $y^2 = x^3 + 9x + 17$ be elliptic curve over $\mathbb{Z}_{23}$ and $P = (16, 5)$ and $Q = (4, 5)$ be two points on the curve. Find $dlog_P Q$. [4 marks]

4. Let $E_{\mathbb{Z}_5} = \{(x, y) \in \mathbb{Z}_5 \times \mathbb{Z}_5 |\ y^2 = x^3 + x + 1\} \cup \{\infty\}$ be an elliptic curve. Show that $E_{\mathbb{Z}_5}$ is a cyclic group and determine its order. [4 marks]

5. Let $E = \{(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11} |\ y^2 = x^3 + x + 6\} \cup \{\infty\}$be an elliptic curve and $P = (2, 7)$ be point on E. Suppose secret keys of Alice and Bob are 2 and 6 respectively. What is the common knowledge using diffie-Hellman key exchange generated by P. [3 marks]

6. Suppose $p = 283$ and $g = 189$, Alice's secret key is $a = 129$. Bob wants to send a message to Alice using ElGamal cryptosystem . So he sends cipher text $(219, 269)$.
   Determine corresponding plain text. [3 marks]

7. Let the prime $p = 73$ and a generator of $\mathbb{Z}_p^*$ be $g = 5$. Find x (by Pohlig Hellman) such that $g^x \equiv 17 \pmod{73}$. [6 marks]

8. (a) Explain Quantum bit and Quantum Entanglement. [2 marks]
   (b) Prove the following three identities.

$$HXH = Z, \quad HYH = -Y, \quad HZH = X$$

   where H represents Hadamard gate, X represent Pauli-X gate, Y represents Pauli-Y gate. [3 marks]
   (c) Let $N = 85$ and $a = 3$ which is coprime to N. Find the non trivial factor of N using Shor's algorithm (calculate the order of 'a' classically). [3 marks]

9. (a) Let $\mathbb{F}_9 = \frac{\mathbb{Z}_3[x]}{\langle x^2+2x-1\rangle}$ be a field of 9 element. Write all the elements of $\mathbb{F}_9$. [1 marks]

   (b) If α is a root of $f(x)$, then find the elements in this field $\frac{\alpha+1}{\alpha-1}$. [2 marks]

   (c) Also find the discrete logarithms of $(\alpha - 1)$ to the base α and α to the base $(\alpha - 1)$. [3 marks]

10. Write the short note (3-5 lines) of the following terms [5 marks]

   (a) Electronic Code Book (ECB)

   (b) Cipher Block Chaining (CBC)

   (c) Cipher Feedback (CFB)

   (d) Output Feedback (OFB)

   (e) Counter (CTR)