Name_____ **Entry No:**_____

Indian Institute of Technology Delhi
Minor-I
MTL-730 (Cryptography)

Time: 1 Hour Max. Marks: 25

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.***

1. (a) Solve the equation $1011x + 2359y = 674$. [1 mark]
   (b) Find 103! under modulo 107. [1 mark]

2. Find four consecutive integers such that each integer has a distinct square factor. [3 marks]

3. (a) Find all factors of 2047 using quadratic seive . [2 marks]
   (b) If the public key for RSA cryptosystem is (2047,35) then decrypt 14. [2 marks]

4. Decrypt the following ciphertext using Rabin cipher ($n = 33$). [4 marks]
   Show all calculations.
   $\mathcal{A} = \{A = 0, B = 1, \ldots, Z = 25, \_ = 26, ? = 27, \ . = 28, @ = 29, ! = 30, \chi = 31, \setminus = 32\}$.

   ?EχQEEQ

5. Decrypt the following Matrix Hill cipher (digraphs) over the alphabets [4 marks]
   $\mathcal{A} = \{A = 0, B = 1, \ldots, Y = 24, Z = 25\}$.

   "IGMMIOEWKO"

   where encryption of **'PART'** is **'YONO'**.

6. Prove or disprove, for a given n such that $n - 1 = 2^s t$, where $s > 0$ and t is an odd integer. Then n passes Miller-Rabin test for a base b if $b^t \equiv 1 \pmod{n}$ or $b^{2^k t} \equiv -1 \pmod{n}$ for $0 \leq k \leq s - 1$. [2 marks]

7. Find all prime divisors of $n = 57$ by Continued Fraction algorithm. (Show all steps)[3 marks]