Name———————————— **Entry No:**————————————

Indian Institute of Technology
Minor 2
MTL-730 (Cryptography)

Time: 1 Hours 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. No marks will be awarded for direct answers. No query will be entertained. Upload your solutions on Moodle . Extra time of 30 minutes is given for uploading.

1. (a) If $n = 493$, find the smallest factor base B such that squares of $27, 29, 31, 32$ are B-numbers and then factor n. [2]
   (b) Show that if $p > 3$ is a prime, then $p^2 \equiv 1 \ (mod\ 24)$. [2]
   (c) Find the factors of $n = 61937$ using Pollard's $(p-1)$ algorithm for factorization. [2]
   (d) Is 126217 a Charmichael number? justify. [2]
   (e) Find the remainder of 180! when divided by 191. [2]
   (f) Apply Robin Miller Primality test to check the primality of 221. [2]
   (g) Let p be an odd prime and let a be a primitive root modulo p. Prove that an integer b has a square root modulo p if and only if its discrete loagrithm $dlog_a b$ modulo p is even. [2]
   (h) Use Fermat's Factorization method to factor 19781. [2]
2. Use Shank's Baby-Step Giant-step alogorithm for discrete logarithm to find: $dlog_5 20$ in $\mathbb{Z}_{47}$. [3]
3. Let $p = 283$, $g = 189$, Alice's secret key $a = 129$. Bob wants to send a message to Alice, so he sends the cipher text $(219, 269)$. Determine the corresponding plain text. [3]
4. Find all solutions of the congruence

$$3x^2 + 5x + 2 \equiv 0 \ (mod\ 2537)$$

[3]