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) Find the factors of $n = 10001$ using Pollard's $(p-1)$ algorithm for factorization. [2]
   (b) Use Fermat's Factorization method to factor 20227. [2]
   (c) If p and q are distinct primes, prove that
   $$p^{q-1} + q^{p-1} \equiv 1 \ (mod\ pq)$$ [2]
   (d) If p and q are distinct odd primes such that $(p-1)|(q-1)$. If $gcd(a, pq) = 1$, then prove that
   $$a^{q-1} \equiv 1 \ (mod\ pq)$$ [2]
   (e) Is 340561 a Charmichael number? justify. [2]
   (f) Find the remainder of 175! when divided by 181. [2]
   (g) Let $n = ab$ where $a, b \in \mathbb{N}$ and $gcd(a, b) = 1$. Then prove that $\phi(ab) = \phi(a)\phi(b)$ where ϕ is Euler's Phi Function. [2]
   (h) 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]
2. Let $p = 53$, $g = 2$, Bob's El-Gamal public key $S = 35$. Alice uses the public key of Bob to generate the cipher text $(37, 24)$. Determine the corresponding plain text. [3]
3. Use Shank's Baby-Step Giant-step alogorithm for discrete logarithm to find :
   $dlog_5 3$ in $\mathbb{Z}_{193}$ [3]
4. If $n = 15251$, find the smallest factor base B such that squares of $121, 123, 124$ are B-numbers and then factor n. [3]