Assignments that you had given to the Mtech CRS batch in your last class(Dated-28/04/2022)

1. Given M is a 2n bit integer and N is a n bit integer, find an algorithm to find M+N, M/N, and the complexity of the algorithm.
2. Given two integers a,n, write a C program to find the inverse of an in mod n if exists(i e, gcd(a,n)=1) and calculate the complexity.
3. Write a c program to implement the square and multiply algorithm.
4. Given a prime p, write an algorithm to find the generator of Zp*.
5. Launch an attack on the Discrete Log Problem.
6. Write down a C code for the primality test algorithm(Solover Strassen; Miller Rabin).
7. Prove the RSA algorithm (Mˆed=M(mod n))
8. If d<Nˆ(1/4) RSA will be broken, Wayner's Algorithm