16 June 2025

Problem Solving Session - II

Given two primes numbers p, q, let $N = pq$.

Question 1: Express $\phi(N)$ in terms of p and q.

Question 2: Suppose N as described above and an $e < \phi(N)$ is given with $gcd(e, \phi(N)) = 1$. Let d be an integer such that

$$ed \equiv 1 \mod \phi(N)$$

Argue that such a $1 \leq d < \phi(N)$ must always exist. Also, give an algorithm that given $\phi(N)$ and e can compute such a d.

Question 3: The factoring problem is as follows: given a composite integer N, obtain two integers a, b such that $N = ab$ with both a and b more than 1. Suppose that we have a (black box) access to an algorithm for factoring.

Let $m \in \mathbb{Z}_N^*$. Suppose that you are given (N, e) and a c which is generated by computing $m^e \mod N$.

Argue that using a black box algorithm for factoring, from (N, e) and c it is possible to recover m.