- You have to discuss the running time of your algorithms. Always try to give algorithm with best possible running time.
- You are required to give proofs of correctness whenever needed.
- You may use any of the following known NP-complete problems to show that a given problem is NP-complete: 3-SAT, INDEPENDENT-SET, VERTEX-COVER, SUBSET-SUM, 3-COLORING, 3D-MATCHING, SET-COVER, CLIQUE.
- **Use of unfair means will be severely penalized.**

There are 3 questions for a total of 30 points.

---

(10) 1. For integers $r, s, r < s$, $s\ (mod\ r)$ is the remainder when dividing s by r. For integers r, s, t, we say that $r \equiv s\ (mod\ t)$ if $r = k \cdot t + s$ for some integer k. For example, $11 \equiv 4\ (mod\ 7)$, $22 \equiv 1\ (mod\ 7)$ etc.

(**RSA**) The RSA public key cryptosystem for private communication can be described in the following manner: Suppose alice wants to send a secret message to Bob. Bob picks two large (1024 bits) prime numbers p and q. Let $N = p \cdot q$. He picks two other numbers $e, d < (p-1)(q-1)$ such that $e \cdot d \equiv 1\ (mod\ (p-1)(q-1))$. Bob makes N and e public (e.g., posts these numbers on his blog) while keeping d secret. Alice who wants to send a message $M \in \{0, ..., N-1\}$ to Bob computes $C \leftarrow M^e\ (mod\ N)$ and sends C to Bob. Bob decrypts it using $M \leftarrow C^d\ (mod\ N)(= M^{ed}\ (mod\ N) = M)$.

Show that if $\mathsf{P} = \mathsf{NP}$, then RSA is *broken*. By broken we mean that an adversary who can see C will always be able to know the secret message M that Alice sends to Bob even without knowing Bob's secret d. You may assume the following:

1. Given $x, p, x < p$, it is easy to find $y < p$ such that $x \cdot y \equiv 1\ (mod\ p)$.
2. It is easy to determine if a given number is prime.

(10) 2. A strongly independent set of a given graph $G = (V, E)$ is defined to be a subset of vertices such that there is no path of length ≤ 2 between any two vertices in this subset. Consider the following problem:

STRONGLY-INDEPENDENT-SET: Given a graph G and an integer k, determine if there is a strongly independent set of size at least k.

Show that STRONGLY-INDEPENDENT-SET is NP-complete.

(10) 3. Consider the following problem:

DEGREE-BOUNDED-INDEPENDENT-SET: Given a graph $G = (V, E)$ with with bounded degree 3 (i.e., all vertices have degree at most 3) and an integer $k < |V|/4$, determine if there is an independent set of G is size at least k.

Either show that DEGREE-BOUNDED-INDEPENDENT-SET is NP-complete or give a polynomial time algorithm for this problem.