CS 581 Homework 10

Due on 03/26/2018 5:00 pm EST

Problem 1.
Consider an RSA key set with $p = 11$, $q = 29$, $n = 319$, and $E = 3$.

a) What value of D can be used in the secret key? Justify your choice.

b) What is the encryption of the message $M = 100$?

c) What message space is provided by this system?

d) Identify all unconcealable messages, and state which depend on this particular choice of E. You may write a small program to help you if you wish.

Problem 2.
Based on the information provided in each of the following scenarios, answer "yes (Y)", "no (N)" or "Unknown (U)" based on what we can conclude about whether A is a member of P, a member of NP, and/or NP-hard. You do not need to justify your answers. Put your answers in the table below. Note that co-P and co-NP are the respective complements P and NP. And no assumption is made whether $P = NP$.

a) B is NP-hard, B $\in NP$ and A $\propto$ B.

b) B is NP-hard, B $\in NP$ and B $\propto$ A.

c) B $\in NP$ and A $\propto$ B.

d) B $\in NP$ and B $\propto$ A.

e) B $\in$ co-NP and A $\propto$ B.

f) B $\in$ co-P and B $\propto$ A.

Question	Is A $\in P$	Is A $\in NP$	Is A NP-hard
a)			
b)			
c)			
d)			
e)			
f)			

Problem 3.
A dominating set for a graph $G = (V, E)$ is a subset D of V such that every vertex not in D is adjacent to at least one member of D. The domination number $\gamma(G)$ is the number of

vertices in a smallest dominating set for G.

Given a graph G and a positive integer p, the decision problem of dominating set is defined as: *is there a dominating set of size p for G?* Suppose we have an algorithm A that can answer "yes" or "no" for a given decision problem of dominating set. Use A as subroutine to solve:

a) The optimization version of dominating set (determine the smallest value of p).

b) The search version of dominating set (find some dominating set of size at most p).