Discrete Structures	Homework 10
CS2800 Spring 2015	RSA, Graphs

1. Suppose that Bob accidentally computes $k^{-1} \mod pq$ instead of $k^{-1} \mod \phi(pq)$ in his implementation of RSA. Show that if he decrypts the message a, he will receive the message $a \cdot (a^t)^{p+q-1}$ for some t.

2. In lecture, we noted that there are several ways to characterize trees (defined as undirected connected graphs with no cycles). For instance, if the undirected graph $G = (V, E)$ is finite (finite numbers of vertices and edges), then any two of the following three properties implies the third.

   Connected: G is connected.

   Acyclic: G has no cycles.

   Sparse: The number of edges is one less than the number of vertices. In brief, $|E| = |V| - 1$.

   We gave short sketches of the proofs. In this homework, we will practice developing and writing out these proofs in detail. Below, we provide an outline of each of the proofs. Write them out properly, emphasizing clarity, precision, readability and completeness. Ensure that every line in your proof is implied by the *preceding* lines (this helps avoid backwards proofs).

   (a) **Connected** and **Acyclic** (that is, the graph is a tree) imply **Sparse**

   First, prove the following subresult:

   > **Lemma 1:** If a tree has at least two vertices, then it must have a vertex of degree 1 (i.e. with only one incident edge).
   >
   > Proceed by contradiction. Assume no vertices have degree 1. Can the tree have a vertex of degree zero? If not, why not? And if all vertices have degree at least 2, and you start walking from vertex to vertex using different edges to enter and exit each vertex, what happens?

   Having proved the lemma, proceed by induction on the number of vertices of the graph. The statement to prove is

   > $S(n)$ = "A tree on n vertices has $n - 1$ edges"

   What is the base case? What is the inductive hypothesis? How can you use the lemma we proved above to prove the inductive step? How should you conclude your inductive proof?

   (b) **Connected** and **Sparse** imply **Acyclic**

   We will first define a *spanning tree*. A spanning tree on graph $G = (V, E)$ is a subgraph of G that is a tree and covers every vertex. In other words, it is a tree (V, E') with $E' \subseteq E$. Note that the spanning tree must cover every vertex, and cannot have edges other than the original ones. A graph need not have a spanning tree, and there may be more than one spanning tree for a graph. Start by proving the following lemma:

   > **Lemma 2:** Every connected graph has a spanning tree.
   >
   > Proceed by induction on the number of edges. First, write down the statement $S(n)$ to be proved. For the base case, if the graph is connected and has zero edges, what can you say about it? Next, write down the inductive hypothesis (remember this is induction on the number of *edges*). For the inductive step, consider two different cases: (i) the graph is a tree, (ii) the graph is not a tree (and hence contains a cycle). The first case should be easy to handle. If the graph does contain a cycle, how can you simplify it so you can apply the inductive hypothesis?

   Now we will wrap up the proof. We are given that G is connected and sparse. Does G have a spanning tree? If so, how can you count the number of edges of the spanning tree? (Hint: use

Q2(a)). Compare this count with the fact that G is sparse to conclude the result (be careful here, the argument is not difficult but you need to write it out precisely!)

(c) **Acyclic** and **Sparse** imply **Connected**

You should be well warmed up from fleshing out the proofs above, so we'll keep the outline brief here. Proceed by contradiction, assuming G is not, in fact, connected. First, prove the following lemma:

> **Lemma 3:** If a graph is not connected, then it can be split into at least two disjoint subgraphs, each of which is connected. (We'll call each such subgraph a "connected component".)

Keeping in mind G has no cycles, what can you say about each of these connected components? Use a result you proved earlier to find the number of edges of the graph as a function of the number of vertices, by summing over the connected components. Show that this value is inconsistent with the relation $|E| = |V| - 1$, leading to a contradiction.