Dalhousie University Faculty of Computer Science
Design and Analysis of Algorithms I
Solution 3 CSCI 3110 Due: 12 Oct 2012

(1) (1.42)
This new cryptosystem is not secure because d can be computed in polynomial time give e, p. Since $\gcd(e, p-1) = 1$, d can be computed in $O(n^3)$ using Extended Euclid Algorithm. The running time is $O(n^3)$ Then we can recover the message by $(M^e)^d \mod p$. However, you need to prove that $(M^e)^d \equiv M \mod p$. Since $ed \equiv 1 \bmod (p-1)$, we have $ed = k(p-1) + 1$. Then $M^{ed} = M^{k(p-1)+1} = MM^{k(p-1)} \bmod p$. Since p is prime, $M^{k(p-1)} \equiv 1 \bmod p$ based on Fermat's little theorem. Therefore $M^{ed} = M^{k(p-1)+1} = MM^{k(p-1)} \equiv M \bmod p$.

(2) Consider a tree T with vertices $V = \{a, b, c, d, e, f, g, h, i, j\}$ and, rooted at a with edges $E = \{(a, b), (b, d), (d, e), (a, c), (c, f), (c, g), (g, h), (g, i), (g, j)\}$.

Find the (undirected) connected graph with the maximum number of edges that has T as its DFS-tree (explain your answer).

DFS-Tree and BFS-Tree T

To find the graph G with the maximum number of edges that has T as its DFS-tree, we begin with $G = T$ and add edges that do not invalidate the DFS-tree. Assume that DFS visits the edges of T in the order they are given above. We can only add an edge (u, v) if u has a higher preorder number then v, or T would not be a valid DFS tree for G. Thus, we add an edge from the node with preorder number i to each node with a preorder number less than i which gives a graph with $9 + \binom{10}{2} = 9 + 45 = 54$ edges. We can also add the forward edges $(a, d), (a, e), (a, f), (a, g), (a, h), (a, i), (a, j), (b, e), (c, h), (c, i), (c, j)$ for a total of $54 + 11 = 65$ edges.

Note:: Figures are (for some reason) are below.

3.2(b) (3 pts) Perform depth-first search on each of the following graphs; whenever there's a choice of vertices, pick the one that is alphabetically first. Classify each edge as a tree edge, forward edge, back edge, or cross edge, and give the pre and post number of each vertex

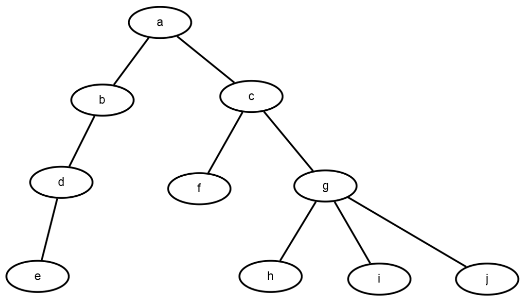
In the graph non-tree edges are shown as dashed lines and are labelled B,C, or F for back, cross, or forward edges. Each vertex is labelled pre:post with its preorder and postorder number.

3.3 (3 pts) Run the DFS-based topological ordering algorithm on the following graph. Whenever you have a choice of vertices to explore, always pick the one that is alphabetically first.

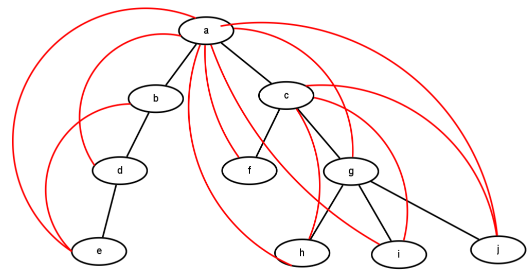
(3) [(a)]

Indicate the pre and post numbers of the nodes.

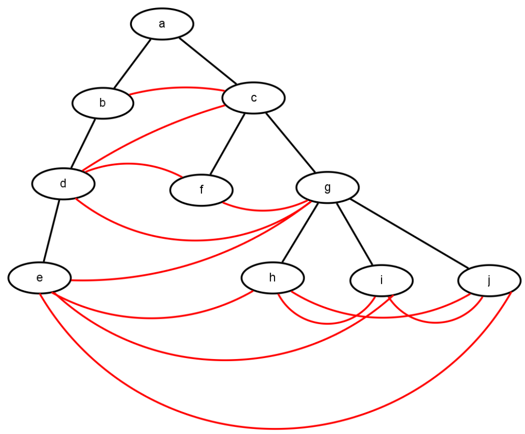
These are shown in the graph as pre:post



(a) (Tree T)



(b) Q1.(a)



(c) Q1.(b)

FIGURE 1. Graphs for Question 2

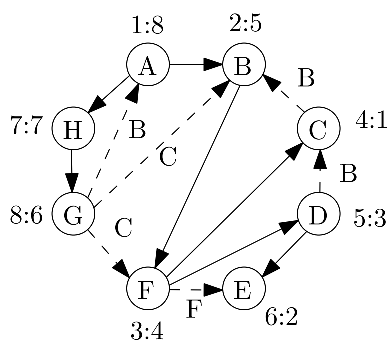


FIGURE 2. Graphs for Question 3

(b) What are the sources and sinks of the graph?

The sources are A and B. The sinks are G and H.

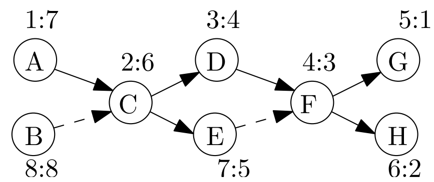


FIGURE 3. Graphs for Question 3

(c) What topological ordering is found by the algorithm?

The topological ordering is B, A, C, E, D, F, H, G.

(d) How many topological orderings does this graph have?

There are three pairs of interchangeable vertices in the ordering, (A, B), (D, E), and (G, H) so there are $2 \cdot 2 \cdot 2 = 8$ possible orderings.

(4) (3.6)

[(a)]Any edge $e = \{u, v\}$, it contributes twice to the degree , i.e., once to u and once to v, therefore, the sum of all degrees is equal to twice the number of edges, namely, $\sum_{u \in V} d(u) = 2|E|$.

Assume there are odd number of vertices whose degree is odd, then we have $\sum_{u \in V}$ is odd. Since $2|E|$ is an even number, $\sum_{u \in V} d(u) \neq 2|E|$, which is contradict to (a). Therefore, there must be even number of vertices whose degree is odd.

Alt Soln:

$$\sum_{u \in V} d(u) = \sum_{odddeg} d(odd - deg) + \sum_{evendeg} d(even - deg) = 2|E|$$

Now, the $R.H.S$ is obviously even, as is the first term on the left (sum of evens is even). This means that the term $\sum\limits_{odddeg} d(odd - deg)$ must be *even*. The only way this can happen is if there is an even number of odd vertices.