CS 1501 Summer 2017 Quiz 2
Wednesday, July 19, 2017

SOLUTIONS

1) **Fill in the Blanks and True/False (20 points -- 2 points each).**
Complete the statements below with the MOST APPROPRIATE words/phrases.

   a) The **Karatsuba algorithm** for integer multiplication improves over the simple divide and conquer algorithm by reducing the number of sub-problems generated at each call from _____**4**_____ to _____**3**_____.
   b) Given a **substitution cipher** on an alphabet with S characters, there are _____**S!**_____ possible keys for the cipher.
   c) When getting a **digital signature** for a message, the "signature" is determined using a _____**cryptographic**_____ hash of the original message.
   d) A graph is stated to be _____ **biconnected** _____ if it has **no articulation points**.
   e) **Breadth First Search** (BFS) on a graph with V vertices and E edges requires in the worst case Theta _____**V + E**_____ using an adjacency list and Theta _____**V^2**_____ using an adjacency matrix.
   f) Given a **heap priority queue** implemented using an array, for index j in the array, parent(j) = _____**j/2**_____ and leftChild(j) = _____**2j**_____.

   Indicate whether each of the following is TRUE or FALSE, **explaining why in an informative way for false answers.**

   g) If someone comes up with an efficient, **polynomial-time factoring algorithm**, the **RSA** encryption scheme will **no longer be useful.** **True**

   h) The **Miller-Rabin Witness algorithm** is used to **verify the authenticity** of sent messages. **False – it is used to test primality.**

   i) **Kruskal's MST** algorithm builds the tree T in the following way: At each iteration pick the best edge joining a vertex in T to a vertex not in T and add the edge and vertex to T. **False – the description is of Prim's Algorithm.**

   j) To do a **deleteMin** operation in a **min-heap**, we remove the root node and replace it with the minimum of its two children. **False – we don't delete the root node at all – rather we copy the last leaf value to the root and delete the last leaf.**

2) **(4 points)** Briefly explain the **key distribution problem**. Be specific as to **why** it is a problem.
Answer: See Powerpoint slide 182. Both sender and receiver need the symmetric cipher key in order to use a symmetric cipher. However, the key must be sent in some secure way from the sender to the receiver. This requires encryption of the key using a different encryption scheme. This requirement continues in a recursive fashion, with no base case.

3) **(8 points)** Consider the PowerMod(X, Y, Z) method which will calculate X^Y mod Z where X, Y and Z are all N-bit integers. Assume that the Gradeschool algorithm is used for integer multiplication. **State and justify** the Theta run-time for the **simple (for loop) solution** for the PowerMod(X, Y, Z) function.
Answer: With the Gradeschool algorithm, each multiplication takes Theta(N^2) time. The number of multiplications required are equal to the value of Y (the for loop will iterate Y times). If Y is an N-bit integer, this value can be up to Theta(2^N). Thus, the total run-time is Theta($N^2 2^N$).

4) **(10 points – 5 + 5)** Consider **RSA encryption**
   a) Show (using pictures and explanation **in detail**) how an **RSA (digital) envelope** works, and **why it is used. NOTE: This is NOT a digital signature!**
   Answer: See Powerpoint slides 201-203

b) Explain the **direct method** for **breaking RSA** that we **discussed in lecture**. Be specific (i.e. mathematical) about the details. Also explain why this is a difficult task for cryptanalysts.
Answer: See Powerpoint Slides 197, 186-187. Breaking RSA directly involves factoring the value N, which is part of both the private and public keys. Once N is factored into its primes (N = XY) we can then determine PHI (= (X-1)(Y-1)). The public key E is already known. Thus the cryptanalyst will have E and PHI and can determine D (the decryption key) by solving the formula ED mod PHI = 1.

Factoring is believed to be an exponential problem, which, for large bit sizes is infeasible to do in a reasonable period of time. Thus, if the keys are large and are not kept for too long, they are quite secure from this attack.

5) **(8 points)** Consider the graph below. Assume the edges are stored in an adjacency list as shown.
<GRAPH REMOVED TO SAVE SPACE – SEE QUIZ FOR GRAPH>

Vertex	Neighbors
A	B, G
B	A, C, E
C	B, D, E
D	C, H
E	B, C, H
F	H
G	A, I, J
H	D, E, F
I	G
J	G

Complete **the table below**, as it would look after a **Depth-First Search Spanning Tree** (starting from vertex A) were created for the graph. `order[]` is the **DFS visit order** for the vertex, and `edgeTo[]` is the **parent vertex** in the DFS tree (ex: if we visit vertex i and then vertex j, `edgeTo[j] == i`) . Show your work above or in the space below the table for partial credit.

	A	B	C	D	E	F	G	H	I	J
order	**0**	**1**	**2**	**3**	**5**	**6**	**7**	**4**	**8**	**9**
edgeTo	**--**	**A**	**B**	**C**	**H**	**H**	**A**	**D**	**G**	**G**