CECS 528, Learning Outcome Assessment 3, Spring 2024, Dr. Ebert

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION ALLOWED. Submit each solution on a separate sheet of paper.

Problem

LO1. Solve the following problems.

(a) Show each of the subproblem instances that must be solved when using the recursive multiplication algorithm for finding the product $x \times y$ for $x = 29$ and $y = 57$. Make sure to provide the solution to each subproblem instance. Hint: there are seven subproblem instances, including the original problem instance as well as the base case instance with $y = 0$.

(b) Consider the RSA key set ($N = 91 = 7 \cdot 13, e = 11$). Determine the decryption key d.

LO2. Solve the following problems.

(a) Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 3T(n/2) + n^{\log_4 16}$. Defend your answer.

(b) Use the substitution method to prove that, if $T(n)$ satisfies

$$T(n) = 3T(n/2) + 5n$$

then $T(n) = \mathrm{O}(n^{\log 3})$.

LO3. Solve each of the following problems.

(a) When analyzing a randomized algorithm, what does $T(n)$ represent with respect to the set of random choices made by the algorithm.

(b) For the `Randomized Quicksort` algorithm, provide an interpretation of the recurrence

$$T(n) = T(6) + T(n-7) + \mathrm{O}(n).$$

What does it mean and under what assumption(s) is it valid?

(c) Recall that the `Minimum Positive Subsequence Sum (MPSS)` problem admits a divide-and-conquer algorithm that, on input integer array a, requires computing the mpss of any subarray of a that contains both $a[n/2-1]$ and $a[n/2]$ (the end of a_{left} and the beginning of a_{right}). For

$$a = 48, -37, 29, -33, 51, -64, 46, -34, 45, -36$$

provide the two sorted arrays $a = \text{LeftSums}$ and $b = \text{RightSums}$ from which the minimum positive sum $a[i] + b[j]$ represents the desired mpss (for the middle), where i in the index range of a and j is within the index range of b. Also, demonstrate how the minimum positive sum $a[i] + b[j]$ may be computed via the movement of left and right markers.