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 $y = 0$.

x	y	xy
29	57	1653
29	28	812
29	14	406
29	7	203
29	3	87
29	1	29
29	0	0

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

We have $(e, (p-1)(q-1)) = (11, (6)(12)) = (11, 72) = 1$

Also,

$72 = (11)(6) + 6$

$11 = (6)(1) + 5$

$6 = (5)(1) + 1$

$6 + 5(-1) = 1$

$6 + (11-6)(-1) = 1 \Rightarrow$

$6(2) + (11)(-1) = 1 \Rightarrow$

$(2)(72 - (11)(6)) + (11)(-1) = 1 \Rightarrow$ $\therefore d = 59$

$72(2) + (11)(-13) = 1 \Rightarrow$

$11^{-1} \equiv -13 \equiv 59 \mod 72$

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.

$n^{\log_2 3} = n^{1+\delta}$ for some $0<\delta<1$

$f(n) = n^{\log_4 16} = n^2 = \Omega\left(n^{1+\delta+\varepsilon}\right)$ for $\varepsilon = 1-\delta$.

$\therefore$ By Case 3 of MT, $T(n) = \Theta(n^2)$

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

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

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

Inductive Assumption: $T(k) \le ck^{\log 3} + dk$ for all $k<n$, and constants $c>0$, and $d \in \mathbb{I}$.

Show $T(n) \le cn^{\log 3} + dn$

$T(n) = 3T(n/2) \le 3\left[c\left(\frac{n}{2}\right)^{\log 3} + \frac{dn}{2}\right] + 5n = cn^{\log 3} + \frac{3dn}{2} + 5n \le cn^{\log 3} + dn \iff \frac{dn}{2} \le -5n \iff d \le -10$

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.

$T(n)$ represents the expected running time, i.e. average number of steps taken by algorithm

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

$$T(n) = T(6) + T(n-7) + O(n).$$

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

Assuming the 7^{th} least member of array a is randomly selected as pivot at the top level of recursion, the expected running time equals $T(6)+T(n-7)+O(n)$, where $T(6)$ is the expected running time for sorting a_{left}, $T(n-7)$ is the expected running time for sorting a_{right}, and $O(n)$ represents the time required to perform the partitioning step.

(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

$$a = \overbrace{\boxed{48, -37, 29, -33, 51}}^{a\text{ left}} \overbrace{\boxed{-64, 46, -34, 45, -36}}^{a\text{ right}}$$

provide the two sorted arrays $a =$ LeftSums and $b =$ 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.

LeftSums = 51, 18, 47, 10, 58

RightSums = −64, −18, −52, −7, −43

a = 10, 18, 47, 51, 58

b = −64, −52, −43, −18, −7

i	j	a[i]+b[j]	MPSS
0	4	3	3
0	3	−8	3
1	3	0	3
2	3	47−18=29	3
2	2	47−43=4	3
2	1	47−52=−5	3
3	1	51−52=−1	3
4	1	58−52=6	3
4	0	58−64=−6	3

MPSS middle