CECS 528, Exam 1, yellow Version, Fall 2023, Dr. Ebert

Rules for Completing the Problems

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION allowed when solving these problems. Make sure all these items are put away BEFORE looking at the problems. FAILURE TO ABIDE BY THESE RULES MAY RESULT IN A FINAL COURSE GRADE OF F.

Directions

Choose up to **six problems** to solve. Clearly mark each problem you want graded by placing an X or check mark in the appropriate box in the Grade(?) row of the table below. **If you don't mark any problems for us to grade or mark 7 or more problems, then we will record grades for the 6 that received the *fewest* points.**

Problem	1	2	3	4	5	6
Grade?						
Result						

Your Full Name:

Your Class ID:

1. Solve each of the following problems. Note: correctly solving these problems counts for passing LO1.

   a. Show each of the subproblem instances that must be solved when using the recursive multiplication algorithm for finding the product xy. Do this for $x = 19$ and $y = 35$. Make sure to provide the solution to each subproblem instance. Hint: there are *seven* subproblem instances, including the original problem instance. (10 pts)

   b. Consider the RSA key set ($N = 65 = 11 \cdot 13, e = 7$). Determine the decryption key d. (15 pts)

2. Solve each of the following problems. Note: correctly solving these problems counts for passing LO2.

   a. Use the Master Theorem to determine the growth of $T(n)$ if it satisfies the recurrence $T(n) = 4T(n/2) + n^{\log_3 9} \log^2 n$. (10 pts)

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

   $$T(n) = 3T(n/2) + n \log n,$$

   Then $T(n) = \mathrm{O}(n^2)$. (15 pts)

3. Solve each of the following problems. Note: correctly solving these problems counts for passing LO3.

   a. Recall that the `Find-Statistic` algorithm makes use of the Partitioning algorithm and uses a pivot that is guaranteed to have at least

$$3(\lfloor \frac{1}{2} \lceil \frac{n}{5} \rceil \rfloor - 2) \geq 3(\frac{1}{2} \cdot \frac{n}{5} - 3) = \frac{3n}{10} - 9.$$

   members of array a both to its left and to its right. Rewrite the above inequalities but now assuming the algorithm uses groups of nine instead of groups of five. Explain your reasoning for each of the numerical changes that you make.

   b. Use Strassen's products $P_1 = a(f-h) = af - ah$, $P_2 = (a+b)h = ah + bh$, $P_3 = (c+d)e = ce + de$, $P_4 = d(g-e) = dg - de$, $P_5 = (a+d)(e+h) = ae + ah + de + dh$, $P_6 = (b-d)(g+h) = bg + bh - dg - dh$, $P_7 = (a-c)(e+f) = ae - ce - cf + af$. to compute the matrix product

$$\begin{pmatrix} 2 & -3 \\ -5 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ -4 & 5 \end{pmatrix}$$

   Show all work. (13 pts)

4. Recall the following recursive multiplication algorithm for multiplying m-bit integer x with n-bit integer y.

   Name: `multiply`

   Inputs: m-bit integer x and n-bit integer y.

   Output: xy.

   Begin

   If $y = 0$, then return 0.

   $z =$ `multiply`$(x, \lfloor y/2 \rfloor)$.

   If y is even, then return $2z$.

   Else return $x + 2z$.

   End

   Determine the worst case running time of this algorithm assuming that

   a. division by 2 requires O(1) steps,
   b. multiplying a k-bit integer by 2 requires $O(k)$ steps and produces a $(k+1)$-bit integer,
   c. adding x to a k-bit integer requires $O(m+k)$ steps and produces a $(\max(k,m)+1)$-bit integer.

   Show all work. (25 pts)

5. Let a, b, m all be positive integers and suppose $(a, m) \mid b$. Prove that the equation

$$ax \equiv b \bmod m$$

has a solution. (25 pts)

6. Consider a problem that takes as input an array a of $n \geq 2$ integers, and a positive integer m that divides evenly into n, i.e. $n = md$ for some positive integer d. The problem is to find the $k = m, 2m, \ldots, (d-1)m$ statistics of a. Provide a high-level description of an algorithm that solves this problem in $O(n \log d)$ steps. Prove that your algorithm achieves the desired running time. Note: credit will not be awarded to descriptions that are ambiguous, make incorrect assumptions/conclusions, and/or do not achieve the desired running time. (25 pts)