CECS 528, Learning Outcome Assessment 4, Yellow, Fall 2023, 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) Evaluate $2^{2^{2023}} \bmod 3$.

(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 $T(n) = 9T(n/3) + n^{\log_4 16} \log^3 n$. Defend your answer.

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

$$T(n) = 4T(n/2) + n \log n$$

then $T(n) = \Omega(n^2)$.

LO3. Solve each of the following problems.

(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 13 instead of groups of five. Explain your reasoning for each of the numerical changes that you make.

(b) Demonstrate the partitioning step of Hoare's version of `Quicksort` for the array

$$a = 4, 8, 1, 6, 2, 7, 5, 3, 9, 11, 10$$

where we assume that the pivot equals the median of the first, last, and middle integers of a.

LO4. Solve each of the following problems.

(a) For n even, state the two properties of the n th roots of unity that allow for a degree-$(n-1)$ polynomial to be recursively evaluated at each of the n th roots of unity in a log-linear number of steps. Hint: you do *not* need to justify your answer. Just state the properties.

(b) Compute $\mathrm{DFT}_4^{-1}(4, -1, 0, 5)$ using the FFT method. Show the solution to each of the subproblem instances (including the original problem instance) that must be solved.