Name: ____

The exam consists of six problems; you only need to solve four. You *must* indicate which four problems you want to have graded by circling the problem numbers — otherwise, I will just grade the first four problems you worked on.

Extra Credit: You may complete a fifth problem for extra credit. Be sure to mark the extra credit problem by circling the problem number and writing "EC" or "Extra Credit" in the margin beside the number.

The following reference materials provided on the last page of the exam: pseudocode for INSERTION-SORT and MERGE-SORT and the statement of the Master Theorem.

- You **have** 120 minutes.
- You **may use only** a calculator, pencil, or pen; you may not use a phone as a calculator.
- You **must** show all calculations. If you fail to show your work, you will receive no credit.
- You **must** put away all notes and papers and close all bags.

(1) Prove the correctness of the main loop of Insertion-Sort (lines 1 – 8).

(2) Derive a recursion for the running time of Merge-Sort and solve the recursion. You may assume that the running time of the Merge function on an n-element subarray is $\Theta(n)$.

(3) The *rod-cutting problem* is as follows. Given a rod of length n inches and a table of prices p_i for $i = 1, 2, \ldots, n$, determine the maximum revenue r_n obtainable by cutting up the rod and selling the pieces. A variant is *rod-cutting with cut cost* in which each cut has fixed cost c. Give a dynamic programming algorithm to solve the rod-cutting with cut cost problem.

(4) Zendian Army bases around the world send encrypted status messages to Army Headquarters on a fixed, known schedule each day: base i sends a status message at time t_i. The Foobarians intercept the messages as they are transmitted and have the ability to attack and decrypt them, but since the different bases use different versions of the encryption machine, the time to attack and decrypt a message depends on the base that sent it: messages from base i take m_i minutes to decrypt. The Foobarians can only attack one message at a time and want to read as many messages as possible. They will only attack a message if they can begin the attack at the time the message is intercepted, otherwise the decrypted message is too old to be of value. Prove that the problem of determining the maximum-size subset of messages that can be decrypted has the greedy choice property and give a greedy algorithm to solve the problem.

(5) Consider an RSA key set with $p = 317$, $q = 277$, and $e = 5$.

a. Find the decryption exponent d using the Extended Euclidean Algorithm and use d to decipher the "message" 21625.

b. Show that $a = 2$ is *not* a witness to the compositeness of p (which makes sense, since p is prime).

(6) The Halting Problem is the problem of determining whether an arbitrary program P with input I will terminate or run forever. Prove that the Halting Problem is NP-hard but *not* NP-complete.

```
Insertion-Sort($A$)
for $j = 2$ to $A.length$
    $key = A[j]$
    // Insert $A[j]$ into the sorted sequence $A[1\,..\,j-1]$.
    $i = j - 1$
    while $i > 0$ and $A[i] > key$
        $A[i+1] = A[i]$
        $i = i - 1$
    $A[i+1] = key$
```

```
Merge-Sort($A, p, r$)
if $p < r$
    $q = \lfloor (p+r)/2 \rfloor$
    Merge-Sort($A, p, q$)
    Merge-Sort($A, q+1, r$)
    Merge(A, p, q, r)
```

Theorem (Master Theorem)**.** *Let $a \geq 1$ and $b > 1$ be constants, let $f(n)$ be a function, and let $T(n)$ be defined on the nonnegative integers by the recurrence*

$$T(n) = aT(n/b) + f(n)$$

where we interpret n/b to mean either $\lfloor n/b \rfloor$ or $\lceil n/b \rceil$. Then $T(n)$ has the following asymptotic bounds:

1. *If $f(n) = O(n^{\log_b a - \epsilon})$ for some constant $\epsilon > 0$, then $T(n) = \Theta(n^{\log_b a})$.*

2. *If $f(n) = \Theta(n^{\log_b a})$, then $T(n) = \Theta(n^{\log_b a} \lg n)$.*

3. *If $f(n) = \Omega(n^{\log_b a + \epsilon})$ for some constant $\epsilon > 0$, and if $af(n/b) \leq cf(n)$ for some constant $c < 1$ and all sufficiently large n, then $T(n) = \Theta(f(n))$.*