MA/CSSE 473 Exam 1 Fall, 2008 Name_____

1. (15) I chose very small numbers for this problem, so the arithmetic can be done without a calculator. Because the possible answers come from a very small set, and could thus be gotten by trial and error, I insist that you show me how you get your answer, in a way that shows that you understand RSA.

   Bob has advertized his RSA public key as (N=33, e=7). Eve intercepts an encoded message, 2. What was the original message?

2. (5) (a) Show how Euclid's algorithm finds gcd(74, 66).

   (5) (b) Find integers x and y such that $74x + 66y = \gcd(74, 66)$

3. (5) (a) If a and b are n-bit positive integers, what is the maximum number of iterations (or recursive calls) made by Euclid's algorithm when calculating gcd(a, b)?

   (5) (b) Prove your result from part (a)

4. (5) What is the discovery made by Carl Gauss that enables the speedup of integer multiplication?

5. (10) Show (using the formal definition of big O) that if $f(x) \in O(h(x))$ and $g(x) \in O(h(x))$, then $f(x)(g(x) \in O((h(x))^2)$

6. (10) Prove Cassini's identity for Fibonacci numbers: $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

   Hint: The left side is the determinant of $\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$. The matrix $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ is relevant.

   Or, you can prove the formula directly, by induction on n.

7. (5) If we use brute force integer multiplication and addition, and brute-force matrix multiplication, what is the big-theta running time (in terms of n) for multiplying n n×n matrices of n-bit integers? Circle one

   $\Theta(n^2)$ $\Theta(n^3)$ $\Theta(n^4)$ $\Theta(n^5)$ $\Theta(n^6)$ $\Theta(n^7)$ $\Theta(n^8)$ $\Theta(n^9)$ $\Theta(n^{10})$ $\Theta(n^{11})$ $\Theta(n^{12})$

8. (10) Name and state the major theorem used for primality testing? Why is using it complicated?

9. (5) Give a big-theta estimate (in terms of n) for the summation $\sum_{i=1}^{n}\sum_{j=1}^{i} ij$ (circle one)

   $\Theta(n^2)$ $\Theta(n^3)$ $\Theta(n^4)$ $\Theta(n^5)$ $\Theta(n^6)$ $\Theta(n^7)$ $\Theta(n^8)$ $\Theta(n^9)$ $\Theta(n^{10})$ $\Theta(n^{11})$ $\Theta(n^{12})$

10. (10) What is the brute force approach to finding the convex hull of a collection of points in the plane? Include a little bit of detail about how the calculation would actually be done.

11. (5) Describe the Knapsack Problem.

12. (5) Five free points!