CSC 464/564 Homework #2 Instructor: Jeff Ward

Covers: Big-O notation; Algorithms with numbers ~~25~~ 20 points

As announced at the end of class on Wednesday, August 31, Problem #4 is being removed from this assignment and will be included on Homework #3.

Solve the following problems:

0.1 (9 points) You do not need to show any work for this problem: just give your answer for each part.

1.13 (5 points) Show your work and support your answer. (Hint: Use Fermat's Little Theorem to determine what the two numbers are modulo 31. Note that 30,000 = 30 · 1,000. Use long division to find 123,456 mod 30.)

Problem #3 (Programming problem; 6 points) Using the programming language of your choice, implement and test the modular exponentiation algorithm from page 19. Use your program to compute 2^{11} mod 10. What answer did you get? (Write it on your homework submission.) Also, upload your program through Canvas.

~~Problem #4 (Calculation problem; 5 points) For this problem, you are free to use the modular exponentiation program that you wrote for Problem #3. Consider the RSA algorithm from Section 1.4.2.~~

~~Suppose Bob chooses p = 131, q = 137, and e = 3.~~

~~What is Bob's public modulus N?~~

~~What is Bob's secret exponent d?~~

~~Suppose Alice wishes to send Bob the message x = 36.~~

~~Derive the encoded message y that she actually sends.~~

~~Show the calculations by which Bob decodes the message.~~