SCI 199 (Beautiful Algorithms)

Assignment #5 Due: Jan. 24, 2002 (in tutorial)

Note: In all questions, the better the algorithm, the better the mark.

1. **[3 marks]** In class we saw the extension of the Euclidean algorithm that allows us to express $gcd(a, b)$ as a linear combination of a and b. Using the language developed in class for describing algorithms, design an implementation of the Extended Euclidean algorithm.

2. (a) **[2 marks]** How should Bob send a signed encrypted message to Alice? Alice must be sure that the message came from Bob. Briefly justify.

   (b) **[EXTRA]** Suppose Alice wants to send an encrypted message M to Bob and wants an acknowledgement that he has received this message. What message can Bob send back to Alice so that she knows that he received M from her? Briefly justify.

3. **[2 marks]** Suppose an RSA scheme is built with $p = 37$, $q = 41$ and thus $n = 1517$. If e is chosen to be 7, what is the value of d? Make sure you use the algorithm presented in class.

4. **[3 marks]** Hand simulate the Modular Power algorithm presented in class to determine $7^{560}(mod\ 561)$. Note that $560_2 = (1000110000)$.