Math 373/578 Homework, Week 8, Due Day 3/7/2012

**Instruction:** In doing this set of problems, you can use any electronic devise to help your computation. But you need to present conclusions based on the analysis of your computation.

1. (Exercise 8.7.4) Alice encrypts a message $m$ with Bob’s public key $(899, 11)$. The ciphertext is 468. Determine the plaintext.

2. Solve the following congruences
   (b) $x^{137} \equiv 428 \pmod{541}$
   (d) $x^{751} \equiv 677 \pmod{8023}$.

3. For each $N = pq$ below, determine the prime factors $p$ and $q$. (Using Matlab to directly find $p$ and $q$ will have zero credits).
   (b) $N = pq = 77083921$ and $(p - 1)(q - 1) = 77066212$.
   (c) $N = pq = 109404161$ and $(p - 1)(q - 1) = 109380612$.

3. Alice chooses two primes $p$ and $q$, and publishes $N = pq$. Alice also chooses random numbers $g, r_1$ and $r_2$ in $\mathbb{Z}_N$ and computes
   $$g_1 \equiv_N g^{r_1(p-1)} \text{ and } g_2 \equiv_N g^{r_2(q-1)}.$$ 
   Her public key is $(N, g_1, g_2)$, and her private key is $(p, q)$.

   Bob wants to send a message $m \in \mathbb{Z}_N$ to Alice. He chooses randomly two number $s_1, s_2 \in \mathbb{Z}_N$ and computes
   $$c_1 \equiv_N mg_1^{s_1} \text{ and } c_2 \equiv_N mg_2^{s_2},$$ 
   and sends $(c_1, c_2)$ to Alice.
   Tell Alice how she can use the Chinese Remainder Theorem to solve the system $x \equiv_p c_1$ and $x \equiv_q c_2$ to find $m$. 

1