Introduction to Cryptology ENEE459E/CMSC498R: Homework 4

Due by beginning of class on 4/24/2014.

1. Exercise 4.14

2. Exercise 4.17

3. Exercise 5.2

4. Exercise 5.5

5. Number theory practice problems:
   (a) Compute $3^{1000} \mod 100$ by hand.

   (b) Compute $[101^{4,800,000,023} \mod 35]$ by hand.

   (c) Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

   Hint: Derive a quadratic equation (over the integers) in the unknown p.

   (d) Let $N = pq$ be a product of two distinct primes. Show that if N and an integer d such that $3 \cdot d = 1 \mod \phi(N)$ are known, then it is possible to compute p and q in polynomial time.

   Hint: Obtain a small list of possibilities for $\phi(N)$ and then use the previous exercise.