Introduction to Cryptology ENEE459E/CMSC498R: Homework 9

Due by beginning of class on 4/23/2015.

1. Compute $3^{1000} \mod 100$ by hand.

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

3. 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 $p$.

4. Let $N = pq$ be a product of two distinct primes. Show that if $N$ and an integer $d \leq \phi(N)$ 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.

5. Fix $N, e$ with $gcd(e, \phi(N)) = 1$, and assume there is an adversary $A$ running in time $t$ for which

   $$\Pr[A([x^e \mod N]) = x] = 0.01,$$

   where the probability is taken over uniform choice of $x \in Z_N^*$. Show that it is possible to construct an adversary $A'$ for which

   $$\Pr[A'([x^e \mod N]) = x] = 0.99$$

   for *all* $x$. The running time $t'$ of $A'$ should be polynomial in $t$ and $||N||$.

   *Hint:* Use the fact that $y^{1/e} \cdot r = (y \cdot r^e)^{1/e}$.