Assignment #2

Due: January 20, 2011

(Corrected 1/15/11 @11am to fix typo in #4)

1. The integer 1 has exactly two distinct square roots: $+1$ and -1. Similarly, whenever p is an odd prime, there are two distinct values x with $0 < x < p$ such that $x^2 \bmod p = 1$: namely $x = 1$ and $x = p - 1$. (Note that when $p = 2$, $p - 1 = 1$, so the two square roots of 1 have the same value.) When $N = pq$ is a product of two distinct odd primes, $x^2 \bmod N = 1$ if and only if both $x^2 \bmod p = 1$ and $x^2 \bmod q = 1$. Since there are two solutions modulo each prime, there are four distinct pairs of solutions modulo p and q: namely (1,1), $(1, q-1)$, $(p-1, 1)$, and $(p-1, q-1)$. Therefore there are four distinct values x with $0 < x < N$ such that $x^2 \bmod N = 1$: one corresponding to each pair of solutions above. Use the Chinese remainder theorem to find the four distinct values of x with $0 < x < 77$ such that $x^2 \bmod 77 = 1$.

2. Suppose that you are given a black box that is capable of computing modular square roots. Specifically, the box takes inputs z and N and outputs a value x such that $x^2 \bmod N = z \bmod N$ if at least one such x exists. (Note that there are many values z that have no modulo N square roots.) Show how you can use this box to efficiently factor any product of two distinct primes. [Bonus: Show how this box can be used to efficiently completely factor into primes *any* integer.]

3. Use induction to prove the corollary of Fermat's Little Theorem given in class (slide 27) that $x^{k(p-1)+1} \bmod p = x \bmod p$ for all primes p and integers k and x with $k \geq 0$.

4. Recall that for any two integers x and y, $x \bmod N = y \bmod N$ if and only if $x - y$ is a multiple of N. Use this fact to show that if p and q are distinct primes and if both $x \bmod p = y \bmod p$ and $x \bmod q = y \bmod q$ are true, then $x \bmod pq = y \bmod pq$ is also true.

5. Combine the results of from Problem 3 and Problem 4 of this assignment to prove the RSA equation: $x^{K(p-1)(q-1)+1} \bmod pq = x \bmod pq$ for all distinct primes p and q and all integers K and x with $K \geq 0$.