# Assignment #6

## Due: February 24, 2011

1. If you know the prime factorization of $N = pq$, it is computationally easy for you to determine whether or not a value $y$ is a square modulo $N$. Describe a process that you can use to convince someone that a given $y$ is *not* a square modulo $N$ *without* revealing the factorization of $N$.

2. Suppose an extremely cautious certificate authority wants to be sure that it only certifies "strong" RSA keys that are the product of two equal-sized primes. Describe a process in which you can engage with the CA at the end of which the CA will be reasonably confident that the key that it certifies is strong but will not know the factorization.

3. A secret $S \in \mathbb{Z}_{101} = \{0,1, \ldots ,100\}$ has been shared amongst five individuals $P_1, P_2, \ldots, P_5$ using Shamir's polynomial-based threshold scheme such that any three of the five can reconstruct $S$. Shareholders $P_1$, $P_4$, and $P_5$ cooperate to reconstruct $S$ and find their respective shares are $(1,37)$, $(4,12)$, and $(5,62)$. What is the secret value $S$? (Be sure that all of your arithmetic – including divisions – are performed modulo 101.)

4. Suppose that you are the fifth of seven shareholders and have receive a share of a secret value $S \in \mathbb{Z}_N$ that has been verifiable shared using the polynomial
$$P(x) = a_3x^3 + a_2x^2 + a_1x + S$$
and committed to with coefficient commitments $A_3 = g^{a_3}$, $A_2 = g^{a_2}$, $A_1 = g^{a_1}$, and $A_0 = g^S$. (Assume that all computations are performed modulo $N$.) You have received the share $(5,13)$. Describe the calculation that you need to perform to verify that your share is valid.