MAT 301 Problem Set 5

[Posted: March 23, 2012. Due: 1pm on April 2, 2012. Worth: 100 points]

Note: I value *succinct* and *clearly written* solutions *without unnecessary verbiage*. Such solutions will be rewarded with bonus points.

1. **Faulty Oracles (50 points)** Let N be an integer, and let e be an integer that is relatively prime to $\phi(N)$. You have access to a faulty oracle that takes as input a number $y \in \mathbb{Z}_N^*$ and return the e^{th} root of y, i.e., a number x such that

$$y = x^e \pmod{N}$$

   There is one little problem though: the oracle can give incorrect answers on as many as half the inputs, namely on half the numbers $y \in \mathbb{Z}_N^*$, it returns an answer $\widetilde{x}$ such that

$$y \neq \widetilde{x}^e \pmod{N}$$

   Moreoever, the oracle can be incorrect on an *arbitrary* set of $|\mathbb{Z}_N^*|/2$ numbers.

   Now, you are given a number $z \in \mathbb{Z}_N^*$ and you are asked to find its e^{th} root mod N. How will you do this efficiently using the faulty oracle? Your procedure should succeed in finding the answer with probability at least $0.9999999999999 \approx 1 - \frac{1}{2^{25}}$.

   [*Note: You don't have the factorization of N, so you can't compute e^{th} roots by yourself efficiently. In other words, you have to rely on the oracle in some way.*]

2. **Secret Sharing (50 points)** Suppose that the teaching staff of a course consists of three professors and two TAs. The solutions to problem sets in the course are encrypted with a key K that is shared between the five staff members. Your goal is to come up with a method of secret-sharing the key so that

   (a) all the three professors together, or
   (b) both the TAs together, or
   (c) any TA together with any professor

   should be able to access the solutions. No other combination of staff members should be able to lay their hands on it (for example, if two professors come together, they should have no idea what the key K is, and therefore, they will not be able to decrypt and figure out the solutions).

   Assume that the key is a number in $\mathbb{Z}_q$ for some prime number q. I will give full points to the solution that minimizes the number of shares (numbers in $\mathbb{Z}_q$) assigned to each staff member.

   [*Hint: Use weights, don't be shy about assigning multiple shares to each person.*]