ASSIGNMENT 1
DUE DATE: Monday 24 September, 2012

This assignment will contribute 8 points towards your final grade.

Consider the variable X that takes integer values between 0 and 1000 (inclusive) according to the following distribution:

Pr(X=0) = 0.01; Pr(X≠0) = 0.00099

The following two methods are used to perturb a particular value x of X.

R₁: x is unchanged with 20% chance, and changed to another number (selected uniformly at random from the remaining possibilities) with 80% chance

R₂: x is changed to x + ξ (mod 1001) where ξ is an integer chosen uniformly at random from {-100, ..., 100}

Q₁ and Q₂ are two properties that an adversary wants to verify, where

Q₁: X=0
Q₂: X is in {200,...,800}

Note that the adversary knows all of this information, except the chosen value of X.

Problem 1 [1 point]:
Show that a 1-to-50 upward privacy breach can occur for Q₁ if perturbation method R₁ is used.

Problem 2 [3 points]:
Show that a 1-to-50 upward privacy breach cannot occur for Q₁ if perturbation method R₂ is used.

Problem 3 [2 points]:
Show that a 50-to-10 downward privacy breach can occur for Q₂ if perturbation method R₂ is used.

Problem 4 [2 points]:
Show that a 50-to-10 downward privacy breach can occur for Q₂ if perturbation method R₁ is used.

Try to submit the solution in class; otherwise slide it under the door of my office by Monday night.