Homework 2: Differential Privacy

For this homework, you will demonstrate knowledge of differential privacy. For all programming parts, you may use basic math and random number generation libraries, but not differential privacy libraries. If in doubt, please contact the professor. Also be sure to submit any instructions for building/compiling/running your code (and keep the process simple).

1. Implement Randomized Response (10 pts)
2. Implement the Laplace Mechanism (10 pts)
3. Implement the Gaussian Mechanism (10 pts)
4. Implement the Exponential Mechanism (10 pts)
5. Read in the supplied csv file and for each column other than the last identify the number of y's from each class. Do this twice, once with ε = 0.01 and δ = 0.05 and again with ε = 1.0 and δ = 0.5. Provide the following in a README or similar document included with your code submission (10 pts).
    a. The true number
    b. The number according to Randomized Response (normal RR with ε = ln(3))
    c. The number according to the Laplace Mechanism (for both values)
    d. The number according to the Gaussian Mechanism (for both values)
    e. The number according to the Exponential Mechanism (for both values)