Please turn in your solution in class on Tuesday 17 March. You are required to work and write your solutions individually.

Question 1

Let $D = \{-1, 1\}$. For each of the following mechanisms on n-row databases over domain D, say if it is "ε-differentially private", "not ε-differentially private but $(\varepsilon, o(1/n))$-differnentially private", or "not $(1, 0.1)$-differentially private". Prove your claim. Assume n is sufficiently large.

(a) Randomly permute the rows of $x \in \{-1, 1\}^n$ and output x.

(b) Choose $y \in \{-1, 1\}^n$ with probability proportional to $\exp(\varepsilon d(x, y)/2)$, where $d(x, y)$ is the number of entries in which x and y differ. Output y.

(c) Sample a $\mathrm{Lap}(1/\varepsilon)$ random variable N. Extend x by $|N|$ entries that equal -1 if $N < 0$ and 1 if $N > 0$. Sort the entries of x (so all the (-1)s come before the 1s) and output x.

Question 2

In this question the database $x \in \{0, 1\}^{n \times n}$ is the adjacency matrix of a simple directed graph G on n vertices. The entry x_{ij} is a 1 if there is an edge from vertex i to vertex j and 0 if not.

(a) Give an ε-differentially private mechanism that answers one in-degree query, that is a query of the type "what is the in-degree of vertex i?" Your mechanism should have accuracy $O(1/\varepsilon)$ with probability 99%.

(b) Show that there is no $(1, 0.1)$ differentially private mechanism for answering an out-degree query with accuracy $0.1n$.

Question 3

Let $D = \{1, \ldots, 10\}$. A *representative* of $x \in D^n$ is an element $a \in D$ that occurs in x, that is $x_i = a$ for some row i.

(a) Design an ε-differentially private mechanism $M \colon D^n \to D$ such that for all $x \in D^n$,

$$\Pr[M(x) \text{ is a representative of } x] \geq 1 - O(e^{-\Omega(\varepsilon n)}).$$

(**Hint:** Consider the number of occurrences of each element $a \in D$ in x.)

(b) Show that if $M(x)$ is a representative of x with probability 1 for all $x \in D^n$ then M is not ε-differentially private for any $\varepsilon > 0$. (**Hint:** Consider databases whose rows are identical.)