Tentative study plan for EEE 6002

Privacy Preserving Machine Learning

Marks Distribution:

Class participation	20%
Midterm project	30%
Final project	30%
Final Exam	20%

Lecture Plan:

Lecture	**Topics**
1-2	Review of common machine learning algorithms
3	Why we need privacy in ML, case studies
4-5	Mathematical definition of privacy, differential privacy, basic building blocks of privacy-preserving algorithm design
6	Midterm presentation
7-8	Privacy for numeric queries, privacy for non-numeric queries
9	Gaussian mechanism
10-11	Composition of multi-stage algorithms
12	Final presentation