6.895 Randomness and Computation	February 8

Course Information
Lecturer: Ronitt Rubinfeld

Lectures: M,W 2:30-4, Room 36-112.

Instructor: Ronitt Rubinfeld, `ronitt@csail.mit.edu`, G32-698, 253-0884.

Teaching Assistant: Matt Menke, `mmenke@mit.edu`, G32-570, 253-4985.

Course Staff: Be Blackburn, `imbe@mit.edu`, G32-692, 253-6098.

Course Website: `http://theory.lcs.mit.edu/~ronitt/COURSE/S06/index.html`

Course topics The course will consist of a subset of the topics mentioned below. The list is subject to change due to my personal whims, class interest and timing issues. The topics will not be covered in the order given below.

- Uses of randomness (examples)
  - Algorithm design:
    - Polynomial zero testing
    - Property testing
    - Small space algorithms for graph connectivity
    - Uniform generation and approximate counting
  - Proofs :
    - Probabilistic proofs
    - Interactive proof systems and probabilistically checkable proof systems
  - Randomness in distributed systems
  - Computational learning theory
- Tools
  - Influence of a variable on a function
  - Random walks on graphs
  - Expander graphs
  - List decoding
  - Fourier representation of a function
  - Sample spaces with limited independence
- Derandomization and pseudorandomness
  - Pseudorandom generators (prg's) based on hard problems

- Randomness from weak random sources
- Randomness extractors
- Extractors vs. prg's
- Techniques for recycling randomness
- Deterministic connectivity in logspace.

Course Requirements Approximately 5-6 homework sets (70%). Scribe notes(25%). Class participation (5%).

Prerequisites 6.045J or 6.046J

Office hours By appointment.