6.875J/18.425J Cryptography and Cryptanalysis September 5, 2001

Handout 1a: Course Information

Instructor: Anna Lysyanskaya *Teaching Assistant: Moses Liskov*

Instructor: Anna Lysyanskaya, `anna@theory.lcs.mit.edu`
Office: NE43-372

TA: Moses Liskov, `mliskov@theory.lcs.mit.edu`
Office: NE43-334
Office Hours: Mondays 3-5pm, in room 34-302.

Course Homepage: `http://theory.lcs.mit.edu/classes/6.875/fall01/`

Topics Covered:

The public-key paradigm
Encryption: indistinguishability, semantic security
One-way functions, trapdoor permutations, and hard-core bits
Pseudorandom generators and functions
Secret-key encryption and MACs
Digital signature schemes
Security against adaptive adversaries for cryptosystems
The random oracle methodology
Secret sharing and threshold cryptography
Commitment schemes
Interactive proofs and zero knowledge

Textbooks: None are required. O. Goldreich, "Foundations of Cryptography" is recommended (available at Quantum Books). S. Goldwasser and M. Bellare, "Lecture Notes on Cryptography" is available free on the web at `http://www-cse.ucsd.edu/~mihir/papers/gb.html`.

Prerequisites: We assume mathematical maturity and familiarity with algorithmic concepts, some number theory, discrete probability, and some complexity theory.

Grading Policy: Your grade will be based on two factors: your problem set grade (P) and your scribe grade (S). The problem set grade will range from 0 to 100 per cent, while the scribe grade will be in a range from 0.8 to 1.2. Your final grade will be calculated as $P \times S$, and letter grades will be assigned from this score.

Scribe Notes: You must scribe at least one lecture, two if the need arises. Scribe notes are due to the instructor two days after the lecture. What we expect for the scribe requirement is for you to give a written summary of the lecture, probably about 4 pages. The scribed lecture must be given in TEX format (we will provide a template).

Homeworks: Problem sets will be due at the beginning of lecture. A limit of 3 extensions will be given to each student during the semester. This is a **firm** policy. *Homeworks will not be accepted late without an extension.*

Collaboration Policy: You may collaborate on solving problem sets, but the write-up of your solutions should be your own. You must list your collaborators.

Note about TEX: It is not required that your homework solutions be type-set but we strongly encourage it. There are great advantages to learning TEX - in addition to being legible and editable, your problem sets will not be losable due to their electronic form. **Moses will be accepting e-mail submission of homework.** The deadline for e-mailed solutions is 11 a.m. on the due date. TEX templates for homework solutions will be distributed via the course web page. The course web page also contains a link to a primer on TEX which should give you most of the TEX skills you need.