MIT EECS COURSE ANNOUNCEMENT

SPRING TERM 2004

6.897 Selected Topics in Cryptography

Instructors:	Ran Canetti and Ronald L. Rivest canetti@theory.lcs.mit.edu, rivest@mit.edu
When/Where:	Thursdays 11:00–12:30 in 36-144, and Fridays 2:30–4:00 in 36-112. First class is 2/5/2004. Note the unusual schedule.
Credit:	3-0-9; Grad-H Credit
Pre-requisite:	6.875 or permission of the instructors.

6.897 is a new graduate course on "selected topics in cryptography"; it emphasizes advanced topics in cryptography related to recent developments in the field.

The details of the course outline are still being worked out, and may depend a bit on who takes the course and what topics they favor. A tentative syllabus for the course is:

- Basic notions of security for cryptographic protocols.
- The universally composable (UC) security framework; UC commitment and ZK; general feasibility results; UC with joint state.
- UC formulations of signatures, key exchange, and secure channels.
- Protocols for electronic voting.
- "Exotic" signature schemes.
- Public-key infrastructures (PKI).
- Concrete security reductions.
- Extractors and privacy amplification.

This course is likely to be a one-time event; it is not likely to become a regular part of the curriculum.

If you are tentatively interested in taking this class, please send email to

`6897s04-staff@lists.csail.mit.edu`

and/or join the mailing list

`6897s04-students@lists.csail.mit.edu`

by visiting the web site

`http://lists.csail.mit.edu/`

If you are interested in the class, but the hours are unworkable for you, please send us mail, with an indication of what hours on Thu/Fri might would work better for you.

See you there!