DIGITAL SCHOLARSHIP LECTURE SERIES

Feb 1st

10:30 am - noon, Newcomb Hall, South Meeting Room

RON RIVEST

**Viterbi Professor of Computer Science,
MIT's Department of Electrical Engineering and Computer Science**

Security of Voting Systems

While running an election sounds simple, it is in fact extremely challenging. Not only are there millions of voters to be authenticated and millions of votes to be carefully collected, counted, and stored, there are now millions of "voting machines" containing millions of lines of code to be evaluated for security vulnerabilities. Moreover, voting systems have a unique requirement: the voter must not be given a "receipt" that would allow them to prove how they voted to someone else---otherwise the voter could be coerced or bribed into voting a certain way. The lack of receipts makes the security of voting system much more challenging than, say, the security of banking systems (where receipts are the norm).

We discuss some of the recent trends and innovations in voting systems, as well as some of the new requirements being placed upon voting systems in the U.S., and describe some promising directions for resolving the conflicts inherent in voting system requirements, including some approaches based on cryptography.

Professor Rivest is the Viterbi Professor of Computer Science in MIT's Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory, and Head of its Center for Information Security and Privacy.

Professor Rivest has research interests in cryptography, computer and network security, and algorithms. Professor Rivest is an inventor, with Adi Shamir and Len Adleman of the RSA public-key cryptosystem, and a co-founder of RSA Data Security. Together with Shamir and Adleman, he received the 2002 ACM Turing Award.

Professor Rivest is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. Professor Rivest serves on the U.S. Election Assistance Commission's Technology Guidelines Development Committee.

ORGANIZING COMMITTEE: Anita Jones - Chair • Bernie Frischer • Matt Neurock • Bill Pearson • Mary Lou Soffa • Tom Skalak • Karin Wittenborg