# Notes for November 2, 2000

1. Greetings and Felicitations!
2. Puzzle of the day
3. Key Exchange
   a. Needham-Schroeder and Kerberos
   b. Public key; man-in-the-middle attacks
4. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
   c. Key Escrow
5. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
6. Types of attacks
   a. Forward searches
   b. Misordered blocks
   c. Statistical regularities (repetitions)
7. Stream ciphers
   a. LFSR: *n* bit register, tap sequence; shift 1 bit right, insert $t_0r_0+...+t_{n-1}r_{n-1}$; can choose period up to $2^n-1$
   b. Self-healing mode
8. Block ciphers
   a. Cipher block chaining
9. Networks and ciphers
   a. Where to put the encryption
   b. Link *vs*. end-to-end
10. Example protocol: PEM
    a. Design goals
    b. How it was done
    c. Differences between it and PGP

# Puzzle of the Day

An educational company is developing a class that will use “distance learning.” The idea is that students can reside at any node on the Internet. The student will download class materials, work independently, and submit the results by electronic mail (or some other prearranged method). During specific times, TAs and the instructor will be on line and available via an interactive conferencing system called Remote Tutor. But there’s one problem: giving tests. The company plans to give interactive tests, with questions being posed and the student answering in real time. The student will be at the remote node, of course.

1. From the company’s point of view, what is the security problem in this scheme? Assume both the connection and the server (to which the test answers are sent) are secure enough so the company is not worried about their compromise.
2. How would you ameliorate the problem?