b. Design goals: drop in (not change), works with any RFC 821-conformant MTA and any UA, and exchange messages without prior interaction
c. Use of Data Exchange Key, Interchange Key
d. Review of how to do confidentiality, authentication, integrity with public key IKs
e. Details: canonicalization, security services, printable encoding (PEM)
f. Certificate-based key management
g. PGP v. PEM

# Notes for March 2, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 377–426; Garfinkel & Spafford, pp. 449–478, 669–700
2. Puzzle
3. Chinese Wall
   a. Theme: market analyst must uphold confidentiality requirements (no use of insider knowledge) but can advise different corporations.
   b. Data items: "objects" (axiomatic), "company datasets" (CD; sets of objects belonging to a company), "conflict of interest classes" (COI; sets of company datasets for companies in competition)
   c. Simple Security Property: Access is only granted if the object requested (a) is in the same CD as an object already accessed by the subject, or (b) belongs to an entirely different COI.
   d. Can derive: if subject accesses object, only other objects in that same CD can be accessed within the same COI. Also, subject has access to at most one CD in each COI.
   e. Sanitization: if it's sanitized then the model does not impose any restrictions.
   f. *-Property: Write access is only granted if (a) access is permitted by the simple security rule, and (b) no object can be read which is in a different CD to the one for which write access is requested and contains unsanitized information.
   g. Can derive: the flow of unsanitized information is confined to its own CD, but sanitized information may flow freely throughout system
   h. BLP: not satisfactory. Say user A accesses company dataset B. But then A is sick, so management has user C do the access. Not possible unless we know for certain C has not accessed anything else in B's COI; BLP doesn't save this info. Also, BLP fixes what datasets a subject can access; the Wall allows dynamic access.
   i. Clark-Wilson: can model it exactly.
4. Network security
   a. Main point: just like a system
5. Review of ISO model
   a. physical
   b. data link
   c. network
   d. transport
   e. session
   f. presentation
   g. application
6. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybel)