Notes for December 6, 1999

1. Greetings and Felicitations!
2. Puzzle of the Day
3. Practise: detecting writing
   a. Integrity check files *à la* binaudit, tripwire; go through signature block
   b. LOCUS approach: encipher program, decipher as you execute.
   c. Co-processors: checksum each sequence of instructions, compute checksum as you go; on difference, complain
4. Network security
   a. Main point: just like a system
5. Review of ISO model
6. Authentication protocols
   a. Kerberos
7. PKI
   a. Certificate-based key management
   b. X.509 model, other models
8. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   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. PGP v. PEM