Notes for January 15, 1997

1. Hello
   a. Would it help to put out code for using getpwnam and getgrent? Gene will discuss this program in section, too.
2. Puzzle of the day
   a. No right answer, but there are better places to look than others. I'll ask this one periodically to see how your knowledge is changing.
3. Breaking UNIX *crypt*(1)
   a. Purely statistical attack is possible (me) but it takes gobs of ciphertext
   b. Known plaintext attack: that's Reeds and Weinberger's attack, with a nice suggestion by Bob Morris
4. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy: (a), given public key, CI to get private key; (b) cipher withstands chosen plaintext attack; (c) encryption, decryption computationally feasible [note: commutativity NOT required]
   c. Benefits: can give confidentiality or authentiction or both