Outline for April 14, 1997

1. Greetings and Felicitations
   a. Remember, talks about what you could do are at the end of this week
2. History
   a. IBM did Lucifer, submitted it in response to NIST CFP
   b. NIST (really, NSA) suggested some minor changes; major one was to make key 56 bits, not 112.
3. Show the cipher
   a. Product cipher with 64 bits in, 64 bits out, and 16 48-bit round keys generated from 56 bit key
   b. Note S-boxes are real heart of algorithm
4. Known attacks and weaknesses
   a. Complementation property: $DES_k(m) = (DES_{k'}(m'))'$ where x' is the bitwise complement of x;
   b. Weak, semiweak keys
   c. If it's a group, multiple encipherment worthless (as group is closed under composition)
   d. differential cryptanalysis: first version unusable as at 16 rounds, more plaintext/ciphertext pairs needed than exhaustive key trial; but for 15 rounds, cuts this time. Later versions cut it to 2^{47} tries. Works by comparing xors of results with xors of corresponding plaintext.. Designers of DES knew about this one, hence the design of the S-boxes
   e. linear cryptanalysis drops required chosen plaintext/ciphertext pairs to 2^{42}; not known to designers of DES.
5. DES Modes
   a. ECB
   b. CBC
   c. note that OFB and CFB exist, essentially use DES as a pseudorandom bitstream generator; OFB feeds back before xor, CFB after
   d. Triple DES and EDE mode