Lecture 7 Notes; April 14, 1997; Notetaker: Scott Miller

DES - Data Encryption Standard

IDEA - cipher following DES correcting some of its problems

Initially IBM created Lucifer
 NSA dropped the key from 128 to 64 bits and claimed it was a good cipher

Takes 64 bits in, ouputs 64 bits
 Key is effectively 56 bits

- is a product cipher - does transposition and substitution
- is a round cipher - algorithm is iterative, run with 16 different keys created from the initial 56 bit key.

Figure on page 16 of the DES handout...

Figure on page 8

Figure on page 11

Attacks against DES
 Complementation property - letter following DES is the key
  DESk(M) = C
  DESe(M') = C'

 Some keys are their own inverses - 4 of them where
  DESo(M) = C
  DESo(C) = M

Double Encipherment gives you nothing
 for keys k1, k2 there is some k3 such that
  DESk2(DESk1(M)) = C is equivalent to
  DESk3(M) = C

Analysis of DES using Differential Cryptanalysis
  Having 16 rounds made this technique basically unusable
  - insight on the NSA's decision...

Modes of DES
  - cypherblock chaining
     link messages xor'd with previous cipher text

  - triple DES (common)
    1) 3 key-triple enciphering
    2) EDE mode
      DESk1(DES^-1k2(DESk3(M)))