Lecture notes for 2.5-2.6 Symmetric encryption

DES (data encryption standard circa 1977)
- Developed by IBM, modified by NSA
  - NSA mods improved resistance to differential cryptanalysis (not known in open community at the time), but weakened key strength
- 64 bit plaintext, 64 bit ciphertext, 56 bit key
- Remaining 8 bits of key often called “check bits”... nonsense... likely weakened by NSA
- 16 round Feistel cipher
- Each round scrambles input of previous round with a 48-bit per-round key
- Key schedule: algorithm to produce 16 per-round keys from 56-bit key
- Each round's substition: S-Boxes
  - Origin is unknown, no backdoors ever found
  - Whenever “magic numbers” appear in an algorithm, cryptographers want to know **why** those numbers were selected

2DES
- C = E(E(P, k1), k2)
- Meet in the middle attack: work forward (2^56) and backward (2^56), overall cost 2^57 even though 112 bits of key

3DES in EDE mode
- C=E(D(E(P, k1), k2), k1)
- Backwards compatible: if k2==k1, then equivalent to DES with k1 (though worse performance)
- Estimated 80 bits of strength (112 bits of key)

3DES in EEE mode
- C=E(E(E(P, k1), k2), k3)
- Estimated 112 bits of strength (168 bits of key)

AES (data encryption standard circa 2001)
- Rijndael algorithm (Dutch)
- 128 bit plaintext, 128 bit ciphertext
  - Key length 128, 192, or 256 bit

Block modes of encryption / decryption

- Use powerpoint slides
- Focus on CBC mode for lecture

Stream modes of encryption / decryption

- Friday's notes has comments for lecture
- Powerpoint slides show how block modes can produce key stream

Time permitting

- Powerpoint slides showing DES operation
- Bring textbook, use overhead projector to show S-Boxes from page 740