Entering the Modern Era of Symmetric Ciphers

Claude Shannon (late 1940’s)

- Alternating layers of substitution and permutation (“confusion” and “diffusion”)
- Build a strong cipher out of weak components!

Two main directions for realizing Shannon’s idea:
- S-P Network (SPN)
- Feistel Network
S-P Network

- Architecture
  - S-boxes
  - Permutations
  - “Ideal cipher”

- Design decisions
  - Block size
  - S-box size
  - S-box contents
  - Permutation(s)
  - Number layers

- Keying
  - Several alternatives

- Design goal: *avalanche effect*
  - Changing any single bit of the input affects every bit of the output
Feistel Network

- Architecture
  - Round function
  - Simplest possible permutation
  - Decryption: invertibility without invertibility!

- Design decisions
  - Block size
  - Number of rounds
  - Round function

- Keying
  - Generation of round keys
  - Use in forward order or reverse order
Data Encryption Standard (DES)

- Creation (IBM + NSA)

- Controversy

- Intense, worldwide analysis (for decades!)

- Importance
DES overall structure
- Feistel network (see Stallings, Figure 3.2)
- Standard specifies $w, n, F, k_i$
- Added to the Feistel network was IP, IP$^{-1}$

Round function F
- (see Stallings, Figure 3.6)
- Expansion permutation E (see Stallings, Table 3.2(c))
- Expanded right half XORed with 48-bit subkey
- Go through what is effectively a 1-round SPN

Row of s-boxes
- S-boxes are not 4x4, but rather 6x4
- (see Stallings, Table 3.3)
- 48 bits of input reduced to 32 bits of output

Permutation P applied to these 32 bits
- (see Stallings, Table 3.2(d))
Subkey generation algorithm
- Start with 64-bit key
- Go through PC1 (now 56 bits)
  - (see Stallings, Table 3.4 (a) and (b))
- Send 28-bit halves through C0 and D0
- Send result through PC2
  - (see Stallings, Table 3.4 (c) and (d))
- Result is XORed with right half data

Full picture of a single round:
- (see Stallings, Figure 3.5)

Full picture of the overall algorithm:
- (see Stallings, Figure 3.4)

DES decryption:
- S-boxes cannot be invertible, so F cannot be invertible
- But, use subkeys in reverse order (Feistel network)
Known Design Criteria for DES

- For the s-boxes:
  - No output bit of any s-box should be too close to a linear function of the input bits
  - Each s-box row should include all 16 possible outputs
  - If two s-box inputs differ in exactly one bit, the outputs must differ in at least two bits
  - If two s-box inputs differ in the two middle bits, the outputs must differ in at least two bits
  - If two s-box inputs differ in their first two bits and are identical in their last two bits, the two outputs must not be the same
  - For any nonzero 6-bit difference between inputs, no more than 8 of the 32 pairs of inputs exhibiting that difference may result in the same output difference

- For the permutation P:
  - The four output bits from each s-box at round $i$ are distributed so that two of them affect “middle bits” of round $i+1$ and the other two affect end bits
  - The four output bits from each s-box affect six different s-boxes in the next round, and no two affect the same s-box
  - For two s-boxes $j, k$, if an output bit from $S_j$ affects a middle bit of $S_k$ in the next round, then an output bit from $S_k$ cannot affect a middle bit of $S_j$
Security of DES

- Reduced-round variants
- Variants with different s-boxes
- Timing attacks
- Differential and linear cryptanalysis
- To date: best attack is exhaustive search of keyspace!
  - Some attempts to increase the key size:
    - DESX; DES-80; 3DES (2-key or 3-key)

Conclusion: very strong cipher with too small a key!

- Complete re-design needed
  - Hopefully increase security while obtaining a smaller, faster cipher

- AES (Advanced Encryption Standard)
Differential and Linear Cryptanalysis

- 1990 and 1993 (respectively)
- Among the most important symmetric cipher attacks known
  - Success against DES
  - Research into improvements / variants
- Essential for a cipher designer to understand these attacks in order to have any hope of building a strong cipher

Note: these are still essentially theoretical attacks against DES, but they have been used to break other ciphers

(see the Tutorial by Howard Heys)