CS 475:Lecture Summary

27th January 2004

Reading: Chapters 2 (for review) and Chapter 3 from the textbook

Review: Last time, we studied some classical symmetric key ciphers such as Caesar, Vigenere, Hill, Vernam and the one-time pad.

Today's Topics:

- Feistel cipher: the basic principles underlying a block cipher.
  1. Basic network.
  2. Shannon characteristics: confusion & diffusion.
  3. Decryption is the inverse of encryption; the keys are used in reversed order.
- Simplified DES
  1. Initial Permutation (IP): 2 6 3 1 4 8 5 7
  2. Expansion/Permutation (E table): 4 1 2 3 2 3 4 1
  3. Substitution/Choice (S-boxes): 2 boxes

     (a) $S_0 = \begin{matrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{matrix}$, $S_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \end{matrix}$

     S-boxes are slightly modified.
  4. Permutation (P): 2 4 3 1
  5. Generation of round keys
     (a) Permuted Choice One (PC-1): 3 5 2 7 4 10 1 9 8 6
     (b) Permuted Choice Two (PC-2): 6 3 7 4 8 5 10 9
     (c) Shift schedule: 2 rounds; left-circular shifts per round (per half).
  6. An example: decrypt 10100010 using key 0111111101; then decode the 8-bit plaintext to 2 letters between A (encoded as 0000) and P (encoded as 1111).
- DES Details: e.g. encrypt (using 1 round of DES) 0123456789abcdef (in hexadecimal) as both plaintext and key.