CS 337 **Quiz 1** **9/29/03**

Open book and notes.

Max points = 50 Time = 50 min Do all questions.

1. (Compression; 11 points)

   (a) (4 points) Create a Huffman tree for symbols with the following frequencies: $\{8, 4, 1, 2, 6, 9, 10\}$.

   (b) (7 points) Show that the successive values computed during execution of the Huffman algorithm (by adding the two smallest values) are nondecreasing.

2. (Error Correction; 21 points)

   (a) (4 points) Let W' be a set obtained from a dependant set W by either removing an element or adding an element. Given W' describe how to determine W.

   (b) (5 points) How many errors can be detected and how many corrected given the following set of codewords: $\{00000,\ 01110,\ 11001,\ 10111\}$?

   (c) (4 points) Given the set of codewords as above, what can the receiver say if she receives the string 01010? What if she receives 10100?

   (d) (8 points) Show that in any Hadamard matrix, the top row has all 1s, and every other row (if any) has equal number of 0s and 1s.

3. (Cryptography; 18 points)

   (a) (7 points) There are 5 candidates in an election; number them 0 through 4. Each voter votes for exactly one candidate and sends its vote to a trusted party. Show that if a voter encrypts his vote directly using public key cryptography, it is vulnerable. Suggest a technique for secure transmission, again using public key cryptography. Show how the trusted party can decrypt and count the votes it receives.

   (b) (4 points) A sender transmits a sequence of blocks using the following scheme. Encrypt the first block by doing exclusive-or of the block with a secret key, and subsequent blocks by doing exclusive-or with the previous encrypted block. Show that this scheme is insecure.

   (c) (7 points) A sender transmits a sequence of blocks using the following scheme. Encrypt the first block by doing exclusive-or of the block with a secret key, and subsequent blocks by doing exclusive-or of the block with the plaintext of the previous block. Show that this scheme is secure if the eavesdropper can only apply exclusive-or over the blocks.

      Hint: Show that no matter how many blocks are exclusive-ored, the result is never a single block of plaintext.