CS 337 **Test 1** **2/21/07**

Open book and notes.

Max points = 75 Time = 75 min Do all questions.

1. (Compression; 28 points)

   (a) (6 points) Create a Huffman tree for symbols with the following frequencies: {12, 8, 20, 6, 32, 4, 20, 24}.

   (b) (16 points) A sender and receiver are using the Lempel-Ziv code. The receiver has built the following trie (same as the one in Page 22 of the notes).

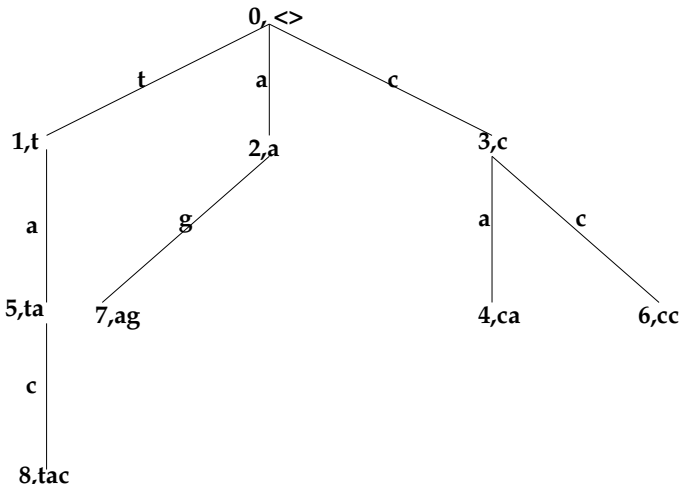

Figure 1: The trie at the receiver using Lempel-Ziv Code

   i. (7 points) Show the sequence of transmissions which resulted in this trie.

   ii. (4 points) What is the string that has been transmitted?

   iii. (5 points) Show the pairs that have to be transmitted for *agtaccag#* given that this trie already exists. You don't have to show the trie at each step; just show the pairs in a table.

   (c) (6 points) Suppose that the string *Ophelia* appears in a text, but the letter O appears nowhere else. How many occurrences of this string should be seen before it is encoded as a word in the Lempel-Ziv coding scheme?

2. (Error Correction; 25 points)

   (a) (5 points) State the necessary and sufficient condition on x, y and z so that $((x + y) \oplus z) < z$?

(b) (10 points) Show that the number of 1s in H_n, the Hadamard matrix of size $2^n \times 2^n$, is $2^{n-1} \times (2^n + 1)$.

(c) (10 points) Suppose 9-bit strings are to be transmitted as 13-bit codes using Hamming code.

i. Prove that the distance between any two codes is at least 3.

ii. Show two such 13-bit codes whose distance is exactly 3.

3. (Cryptography; 22 points)

(a) (8 points) Compute $36^{36} \bmod 11$. Show the steps. Use modular simplification rule and other rules about mod.

(b) (7 points) Bob's public key is the pair $(3, 355)$. What is his private key?

(c) (7 points) Alice's public key is the pair $(1, n)$, for some n. Is there a problem with this choice? Suppose $(1, n)$ is the private key. What is the public key, and is there a problem with this choice?