CS 337 **Test 1** **2/20/08**

Open book and notes.

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

1. (Compression; 25 points)

   (a) (3 points) What is the entropy of an alphabet of 16 equiprobable symbols?

   (b) (6 points) Create a Huffman tree for symbols with the following frequencies: {1, 1, 2, 3, 5, 8, 13}. What is its weight?

   (c) (16 points) A sender and receiver are using the Lempel-Ziv code. The receiver has built the following trie.

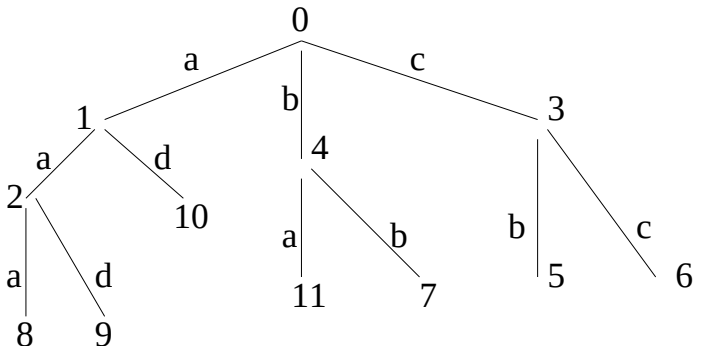

Figure 1: The trie at the receiver using Lempel-Ziv Code

   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) Given that this trie already exists, show the pairs that have to be transmitted for the string *cbcbbabbbcbacbbbbc#*. You don't have to show the trie at each step; just show the pairs in a tabular form.

2. (Error Correction; 28 points)

   (a) (5 points) Modify oblivious communication to work when Alice has 4 data items. Specify the steps for Alice, Bob and Charles. Argue correctness.

   (b) (8 points) In the game of Nim, consider a winning configuration for the first player. Can the the first player always remove from the largest pile and still have a winning strategy? When can he remove an entire pile (and still have a winning strategy)? Justify your answers.

(c) (5 points) Alice has the following string to transmit: 10011001110. She uses Hamming code to add check bits. What does she actually transmit?

(d) (6 points) How many errors can be detected and how many corrected given the following set of codewords: {11111, 10001, 00111, 01000}?

(e) (4 points) Given the set of codewords as above, what does the receiver decode the string 10101? What if he receives 01011?

3. (Cryptography; 22 points)

(a) (7 points) A number of bidders are bidding for an item at a website like eBay. Assume that all the bids are expected to be below $100, and the bids are in whole dollar amounts. For obvious reason, no bidder would like his bid to be read by any unauthorized party. Show that if a bidder encrypts his bid directly using public key cryptography, it is vulnerable.

To overcome the vulnerability, suggest a policy that eBay can proclaim publicly.

(b) (7 points) Compute $79^{62} \bmod 7$. Show the steps. Use the rules given in the class for manipulating such expressions.

(c) (8 points) Alice's public key is the pair $(7, 155)$. What is her private key?

Hint: You don't have to use the extended Euclid algorithm. Solve the appropriate equation using inspection.