1. (Compression; 14 points)
   (a) (6 points) Create a Huffman tree for symbols with the following frequencies: {6, 4, 10, 3, 16, 2, 10, 12}.
   (b) (8 points) A sender sends the following sequence of transmissions using Lempel-Ziv Code:
       
       (0, p), (0, q), (0, r), (3, q), (0, s), (1, q), (3, r), (2, s), (6, r), (4, r), (6, #)

       As usual, index 0 refers to a null string. Show the table (the dictionary) the receiver builds from these transmissions. What is the string that is sent? You don’t have to show the trie.

2. (Error Correction; 23 points)
   (a) (5 points) Given are two non-empty sets, \(L\) and \(R\), of words (binary strings of equal lengths). Suppose \(\hat{L} = \hat{R}\). (Recall \(\hat{L}\) is the exclusive-or of all the words in \(L\)). A subset of \(L\) is removed from \(L\) and added to \(R\), and independently a subset of \(R\) is removed from \(R\) and added to \(L\), resulting in sets \(l\) and \(r\). Show that \(\hat{l} = \hat{r}\).
   (b) (6 points) How many errors can be detected and how many corrected given the following set of codewords?
       \{11111111, 11001100, 10011001, 10010110\}
   (c) (4 points) Given the set of codewords as above, what can the receiver say if she receives the string 11001000? What if she receives 11011101?
   (d) (8 points) Take any Hadamard matrix \(H_n\). You may apply the following operations to it in any order as many times as you like: (1) complement all the bits in a row (replace all 0s by 1s and vice versa), (2) complement all the bits in a column, (3) exchange any two rows, and (4) exchange any two columns.

       Show that in the resulting matrix the Hamming distance between any two distinct rows is \(2^{n-1}\). You may assume that the Hamming distance between any two distinct rows in \(H_n\) is \(2^{n-1}\).

       Hint: Think in terms of invariant.

3. (Cryptography; 13 points)
   (a) (6 points) Compute \(23^{28} \mod 7\). Show the steps. We have discussed how to simplify such expressions without the use of a calculator.
(b) (7 points) A sender transmits a sequence of blocks using the following scheme. Encrypt the first block by doing exclusive-or of its plaintext with a secret key, and subsequent blocks by doing exclusive-or of the plaintext 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 encrypted blocks.

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