Say that you have a cryptosystem with two plaintext messages m_0 = "The British are coming" and m_1 = "The sky is falling" that each occur with probability 1/2. Also say that there are 4 keys which are equally likely k_0, k_1, k_2, k_3 which send the plaintext messages to one of the four cyphertexts

$$c_0 = \text{"cheese sandwiches."}$$
$$c_1 = \text{"milk and cookies"}$$
$$c_2 = \text{"mashed potatoes"}$$
$$c_3 = \text{"Ted Danson."}$$

Say that message m_i will be sent under key k_j to the cyphertext $c_{2i+j(mod4)}$.

(a) It is agreed in advance that today key that is being used is k_2. You receive the message "mashed potatoes." What plaintext does this represent?
(b) Does this system achieve perfect secrecy? Why or why not?
(c) Compute $H(K|C)$.
(d) Now assume that the 4 keys are not chosen with equal probability and instead k_0 and k_2 are chosen with probability 1/8 and k_1 and k_3 are chosen with probability 3/8. Does this system achieve perfect secrecy? Why or why not?
(e) Under this new system calculate $H(K|C)$.

Suppose you are to write a program to simulate the output of a fortune wheel producing 1 2 3 4 5 6 with respective probabilities

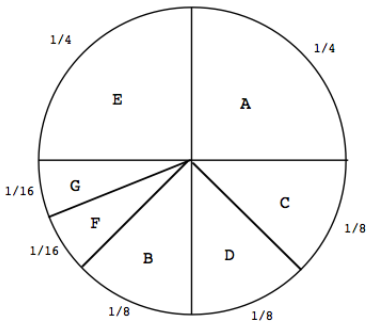
1/8 1/8 1/4 1/6 1/6 1/6

Suppose you have already written a random number generator yielding a random variable W uniformly distributed in [0,1] and that the only thing missing in your program is the procedure which converts W into one of the numbers 1 2 3 4 5 6. Draw the decision tree that carries out this conversion with the smallest expected number of comparisons.

A candy maker manufactures 7 chocolate Easter bunnies of increasing sizes. His plan was to use 10 grams of chocolate for the first and 10 additional grams for each of the successive ones. So, at the end, the bunnies should have weighted 10, 20, 30, 40, 50, 60 and 70 grams respectively. However, he takes a lunch break after making the first k and during that time a mischievous helper messes up his scale so at the end the remaining $7 - k$ end up weighing 10 grams more than they should have. Suppose that you are to determine after which bunny he went to lunch by means of a scale with outputs <, =, or >

a) What is the minimum number of weighings you need to determine k?
b) Construct a scheme of weighings which achieves this minimum.

Suppose that a certain message $X_1, X_2, X_3, \ldots, X_N$ is obtained by successive spins of the fortune wheel given on the right.



(a) Determine the minimum number of binary registers you need on the average to store such a message.
(b) Using the tree from heights and trimming any incomplete branches, construct a comma-free encoding of the letters A, B, C, D, E, F, G into binary strings that will enable you to store the message.
(c) Using the tree constructed in the previous question, calculate the expected number of bits per register necessary to encode this file.