(1) 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 $H(K|C)$.

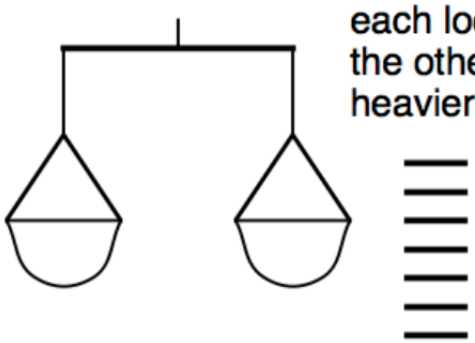
(2) Calculate the unicity distance of the Vernam cipher with $p = 7$ and $q = 5$ (the lengths of the two keys). Use the table from the notes to estimate the entropy of English and assume that all keys are equally likely.

1. In the enciphering system MIX45 the message is first Vigenere encrypted with a 4-letter keyword, and then subjected to a rectangular transposition of period 5. Determine the unicity distance of MIX45. Assume all ciphers are equally likely.

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 scale compares weights, testing if two objects weigh the same, the left is heavier, or the right is heavier. There are seven coins, each look the same but one of the seven is heavier or lighter than the others. Draw the decision tree that determines which is the heavier or lighter coin in a minimum number of weighings.