(1) Say that you have a cryptosystem with 4 messages m_0, m_1, m_2, m_3 which are not equally likely, in fact they are known to be sent with probabilities $1/5, 1/5, 3/10, 3/10$. Two keys are used k_0 and k_1 which are both equally likely where m_i is mapped to $c_{i+j \mod 4}$ under key k_j where $i \in \{0, 1, 2, 3\}$ and $j \in \{0, 1\}$
   (a) (2 points) Does this system achieve perfect secrecy? Why or why not?
   (b) (2 points) Calculate $H(K|C)$.

(2) Say that you have a cryptosystem with 2 messages m_0, m_1 which occur with probability $1/4$ and $3/4$ and 4 keys which k_0, k_1, k_2, k_3 which are equally likely. This time, m_i is mapped to $c_{ij+j \mod 4}$ under key k_j where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3\}$.
   (a) (2 points) Does this system achieve perfect secrecy? Why or why not?
   (b) (2 points) Calculate $H(K|C)$.

(4) A random procedure for choosing a three letter word is determined from the charts below and the outcome is a random variable X. The first letter is chosen with probability given by the first table, the second and third letters are chosen using the table below where the entries represent the the number of times the second letter appears (in the column) given the previous letter (in the row).

a	4
s	2
d	1
f	3

	a	s	d	f
a	5	0	2	3
s	2	4	4	0
d	1	5	3	1
f	6	1	1	2

   (a) (2 points) Find $H(X|$ the third letter is 'f')
   (b) (2 points) Encode the set of three letter words that end in an 'f' by using a Huffman tree with one word per leaf of the tree.
   (c) (2 points) What is the expected number of bits required to store a single word using this coding scheme?

(2) A substitution cypher is used where each plaintext is grouped into 2-grams and each 2-gram is replaced by another 2-gram according to a 26×26 table. In other words, each key consists of a matrix 26×26 entries where each entry is a different 2 letters (no 2-gram appears twice in the table).
Assume that the entropy of English for your message is 1.2 bits per letter and that all cyphertexts and keys are equally likely. Calculate the unicity distance of this cypher system.
Hint: it will be difficult to calculate H(K) on your calculators. Just leave the result as an expression.

(3) What is the unicity distance of the homophonic encryption system with key length 20? You may assume that entropy of English is 1.5 bits of information per letter.