1) $S = \{ \overset{Pr(s) = 0.15}{A_1}, \overset{0.2}{A_2}, \overset{0.25}{A_3}, \overset{0.4}{A_4} \}$

$\Rightarrow H(S) = -\sum_{s \in S} Pr(s) \log_2 [Pr(s)] \approx 1.904$

2) See attached excel sheet

3) a) See excel sheet
   b) " "

1. What is the entropy (average information) of a source that produces 4 distinct alphabets with probability 0.15, 0.2, 0.25 and 0.4 respectively?
2. The purpose of this problem is to show the unbreakability of the one-time pad. Suppose we are using the shift cipher with 27 characters (you do mod 27 instead of mod 26) in which the twenty-seventh character is the space character. However, you use a different key for each alphabet so that in effect you have a one-time key that is as long as the message. Given the ciphertext
   ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
   find the key that yields the following plaintext:
   MR MUSTARD WITH THE CANDLESTICK IN THE HALL
   and find another key that yields the following plaintext:
   MISS SCARLET WITH THE KNIFE IN THE LIBRARY
   Comment on the result. Is it possible to find a third key that gives you the sentence MEET ME ON FRIDAY AT SIX PM? You may use a modification of the program from HW1 to solve this problem.
3. The S-boxes in DES must be non-linear to make DES secure. Show that $S_2(x_1) \oplus S_2(x_2) \neq S_2(x_1 \oplus x_2)$ and repeat the same for S_5 where:
   a. x1 = 000000 and x2 = 111111
   b. x1 = 111111 and x2 = 111111
4. DES encrypts 64 bit blocks of data. Assume a DES chip can encrypt two blocks of data in three clock cycles. (a) What is the clock frequency required to encrypt an ATM network link running at a speed of 155.52 Mb/s? (b) What is the clock frequency required, if four rounds of DES take three clock cycles? Ignore the time taken by IP and IP^{-1} for the latter case.
5. Suppose we have an enhanced version of DES that uses 128 bit keys instead of 56 bit keys.
   a. If a DES chip can do three decryptions in five clock cycles and it is clocked at 4 GHz, compute the average and worst case time (in years) required to do a brute force attack with a known plaintext. How does this compare with the age of the earth which is estimated to be 4.55 billion years?
   b. If the chip speed doubles every 18 months (Moore's Law), how many years do we have to wait before this enhanced version can be broken by brute force in 24 hours? How do the results change if 10000 chips run in parallel in each case? Compare the times and comment on the results.
6. Dan claims that he can use DES without the initial permutation and its inverse with the same level of security as he would have with the two operations. Argue why his claim is true or false. Show all steps in your explanation.

Definition 2.4: Suppose **X** is a discrete random variable which takes on values from a finite set X. Then, the *entropy* of the random variable **X** is defined to be the quantity

$$H(\mathbf{X}) = -\sum_{x \in X} \mathbf{Pr}[x] \log_2 \mathbf{Pr}[x].$$

4) Chip can encrypt 2 blocks (128 bits) in 3s w/ s = 1 cycle.
   a) freq req'd for 155.52 Mb/s (Mega byte) encryption?
   Ans: $128/3 \approx 42.67$ bits/cycle = chip encryption speed

   $$\frac{(8)(1e^6)(155.52) = 1.244e9 \text{ bit/s}}{(128/3 \text{ bits/cycle})} \Rightarrow \text{freq req'd is } 29{,}160{,}000 \text{ Hz (cycles/s)} \approx 29.16 \text{ MHz}$$

   b) 14,580,000 Hz ≈ 14.58 MHz, see attached

5) a) 9.87e11 times the age of earth, see attached work
   b) $4E9 \text{ Hz} \times 2^x = 6.56E33 \text{ Hz} \Rightarrow x = \log_2\left(\frac{6.56E33}{4E9}\right) = 80.44$ doubles
   $\Rightarrow$ 120.661 yrs, $\Rightarrow$ 100.73 yrs w/ 10,000 parallel chips, not much better.

6) True,