1.

A Differential Cryptanalysis attack will involve testing different input pairs and comparing the difference in their outputs. To start, the first thing we need to do is generate our distribution table. We do this by passing all possible input pairs through S-box S0, storing the xor of the pairs and the xor of S-box output. The result will be a 16x4 table of values to use for possible keys.

Next, we need to calculate potential key values. We know that S0 is unbalanced; it contains more 3's than any other number. As a result, the inputs we choose to test should have an S-box output xor value of 3. So take the pair of values whose s-box output xor'ed to 3, and xor one of those values by all other input pairs that xor'ed to 3. This process will give us one set of potential keys.

Finally, we repeat the above process, using a difference pair of inputs whose S-box output also xor's to 3. The intersection between the resulting potential key sets yields the actual key value.

2.

Compute probabilities P_c

$$P_c(1) = \frac{1}{2} * \frac{1}{3} + \frac{1}{2} * \frac{1}{4} = \frac{7}{24}$$

$$P_c(2) = \frac{1}{2} * \frac{1}{6} + \frac{1}{2} * \frac{1}{2} + \frac{1}{4} * \frac{1}{3} = \frac{5}{12}$$

$$P_c(3) = \frac{1}{4} * \frac{1}{6} + \frac{1}{4} * \frac{1}{3} = \frac{1}{8}$$

$$P_c(4) = \frac{1}{4} * \frac{1}{6} + \frac{1}{4} * \frac{1}{2} = \frac{1}{6}$$

Also compute H(K) + H(P)

$$H(K) = -\left(\frac{1}{2} log_2 \frac{1}{2} + \frac{1}{4} log_2 \frac{1}{4} * 2\right) = 1.5$$

$$H(P) = -\left(\frac{1}{3} log_2 \frac{1}{3} + \frac{1}{6} log_2 \frac{1}{6} + \frac{1}{2} log_2 \frac{1}{2}\right) = 1.46$$

Now plug in P_C to get H(C)

$$H(C) = -(\frac{7}{24} \log_2 \frac{7}{24} + \frac{5}{12} \log_2 \frac{5}{12} + \frac{1}{8} \log_2 1/8 + \frac{1}{6} \log_2 \frac{1}{6}) = 1.85$$

Finally evaluate H(K) + H(P) – H(C)

H(K|C) = 1.5 + 1.46 – 1.85 = 1.11