1. Based on the definition of the attack, we assume that the adversary has the ability to pick plaintext and see the cyphertext associated with it. Assuming their knowledge of the inner workings of the algorithm structure, they can then pick plaintext pairs that have XORs and find their corresponding cyphertext pair XORs. Using this method that could then build a table of said XORs called a differential distribution table in order to find a plaintext XOR that only has one cyphertext XOR related to it.  
     
   Assuming that the differential distribution table given in the slides for S0 is accurate, then the table cell X’ of 7 ---> Y’ of 1 has only 2 solutions which should be effectively 1 symmetric pair.  
     
   With some math, we find the inputs 1 and 6 would be these numbers. Proof: 1 XOR 6 = 0001 XOR 0110 = 0111 = 7. And S0(1) XOR S0(6) = 3 XOR 2 = 11 XOR 10 = 01 = 1  
     
   Now, for assume the convenient hypothetical that the adversary knows that the input of 2 and 5, which also XOR to 7, happen to have an output XOR of 3. Through the process of building the table, that adversary would also naturally be aware of the possible input values that XOR to 7 but have an output XOR of 3, let’s call this set T. From here the possible keys for this position is reduced to 2 XOR t for all t within T and 5 XOR t for all t within T. Rinse and repeat to continue narrowing down possible keys.
2. H(K|C) = H(K) + H(P) - H(C)  
     
    = -{(½)log2(½)+(¼)log2(¼)+(¼)log2(¼)} + H(P) - H(C)  
     
    = -{(½)log2(2-1)+(¼)log2(2-2)+(¼)log2(2-2)} + H(P) - H(C)  
     
    = -{(½)(-1)+(¼)(-2)+(¼)(-2)} + H(P) - H(C)  
     
    = -{-(½) - (½) - (½)} + H(P) - H(C)  
     
    = (3/2) - {(⅓)log2(⅓) + (⅙)log2(⅙) + (½)log2(½)} - H(C)  
     
    = (3/2) - {(⅓)log2(⅓) + (⅙)log2(⅙) + (½)log2(2-1)} - H(C)  
     
    = (3/2) - {(⅓)log2(⅓) + (⅙)log2(⅙) + (½)(-1)} - H(C)  
     
    = (3/2) - {(⅓)log2(⅓) + (⅙)log2(⅙) - (½)} - H(C)  
     
    = (3/2) - {-1.45914} - H(C)  
     
    = (3/2) - {-1.45914} - H(C)  
     
    = (3/2) + {1.45914} - [- {(7/24)log2(7/24) + (¼)log2(¼) + (⅛)log2(⅛) + (⅙)log2(⅙) } ]  
     
    = (3/2) + {1.45914} - [- {(7/24)log2(7/24) + (¼)(-2) + (⅛)(-3) + (⅙)log2(⅙) } ]  
     
    = (3/2) + {1.45914} - [- { -1.82429 } ]  
     
    = 1.13485  
   1. Pc(1) = (⅓)(½) + (½)(¼) = (4/24) + (3/24) = (7/24)
   2. Pc(2) = (⅓)(¼) + (⅙)(¼) + (½)(¼) = (2/24) + (1/24) + (3/24) = (6/24) = (¼)
   3. Pc(3) = (⅓)(¼) + (⅙)(¼) = (2/24) + (1/24) = (3/24) = (⅛)
   4. Pc(4) = (⅙)(¼) + (½)(¼) = (1/24) + (3/24) = (4/24) = (⅙)