Jack Dates

1. The sbox takes in 4bit values and outputs 2bit values. There are then $2^4=16$ possible inputs. If we consider all 256 input pairs, we can calculate their xor and their substitutions' xor to build a differential table: (generated programmatically)

S_0 differential distribution

input xor	output xor 0	1	2	3
0	16			
1	8		8	
2		16		
3		8		8
4			16	
5	8		8	
6				16
7		8		8
8	8		8	
9	8		8	
a		8		8
b		8		8
c	8		8	
d	8		8	
e		8		8
f		8		8

This is a non uniform distribution. We can also keep track of the actual input pairs that generated the outputs. Now suppose we know an input pair (3, 4) with input xor 7 and that their outputs from S_0 have xor 1. The mapping $7 \to 1$ has as possible sbox input pairs: (0,7) (1,6) (2,5) (3,4). The input to S_0 is $S_I = S_E \oplus S_K$ where S_E is the permuted input and S_K is the round key. Rearranging gives $S_K = S_I \oplus S_E$. We know S_E is one of (3,4) and S_I is any of (0,7,1,6,2,5,3,4). Enumerating all combinations:

$0+3=3$ $7+3=4$ $1+3=2$ $6+3=5$ $2+3=1$ $5+3=6$ $3+3=0$ $4+3=7$

$0+4=4$ $7+4=3$ $1+4=5$ $6+4=2$ $2+4=6$ $5+4=1$ $3+4=7$ $4+4=0$

so S_K is one of (0, 1, 2, 3, 4, 5, 6, 7)

The total possible keys that contribute to the 4bit input to S_0 is $2^4=16$, so we have halved the space by finding only 8 possibilities here. If we continued with more input/output pairs we could eventually find the key.

2. Theorem: $H(K|C) = H(K) + H(P) - H(C)$

$$H(K) = -\left(\tfrac{1}{2}\log_2\tfrac{1}{2} + \tfrac{1}{4}\log_2\tfrac{1}{4} + \tfrac{1}{4}\log_2\tfrac{1}{4}\right) = -\left(-\tfrac{1}{2} - \tfrac{1}{2} - \tfrac{1}{2}\right) = \tfrac{3}{2}$$

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

$$P_C(1) = \tfrac{1}{3}\cdot\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{4} = \tfrac{7}{24}$$

$$P_C(2) = \tfrac{1}{3}\tfrac{1}{4} + \tfrac{1}{6}\tfrac{1}{2} + \tfrac{1}{2}\tfrac{1}{2} = \tfrac{10}{24}$$

$$P_C(3) = \tfrac{1}{3}\tfrac{1}{4} + \tfrac{1}{6}\tfrac{1}{4} = \tfrac{3}{24}$$

$$P_C(4) = \tfrac{1}{6}\tfrac{1}{4} + \tfrac{1}{2}\tfrac{1}{4} = \tfrac{4}{24}$$

$$H(C) = -\left(\tfrac{7}{24}\log_2\tfrac{7}{24} + \tfrac{10}{24}\log_2\tfrac{10}{24} + \tfrac{3}{24}\log_2\tfrac{3}{24} + \tfrac{4}{24}\log_2\tfrac{4}{24}\right) \approx 1.85$$

$$H(K|C) = 1.5 + 1.46 - 1.85 = \boxed{1.11}$$