Nick Roper

1)
Consider two inputs x and x^* to Sbox S_0 with outputs y and y^* (i.e. $y = S_0(x)$ and $y^* = S_0(x^*)$).
Let $x' = x \oplus x^*$ and $y' = y \oplus y^*$.
Find all pairs of inputs to S_0 that xor to x' and whose outputs xor to y'.
xor each of these inputs by x and x^* to create a set of possible subkeys.
Restart this process with different x and x^* until the number of possible subkeys is only 1, and then this must be the subkey being used for S_0.

For example, suppose the subkey 13 is being used.
Let $x = 5$ and $x^* = 6$. Thus, $x' = 3$.
After each is xor'ed by the subkey and S_0 is used, we find that $y = 0$ and $y^* = 1$, so $y' = 1$.
We find all pairs of inputs to S_0 satisfying that $x' = 3$ and $y' = 1$: these are $\{8, 9, 10, 11\}$.
Then, we xor each of these with x to get a new set of possible subkeys $\{12, 13, 14, 15\}$.
Starting again, let $x = 4$ and $x^* = 11$. Thus, $x' = 15$.
After each is xor'ed by the subkey and S_0 is used, we find that $y = 3$ and $y^* = 2$, so $y' = 1$.
We find all paits of inputs to S_0 satisfying that $x' = 15$ and $y' = 1$: these are $\{6, 9\}$.
Then, we xor each of these with x to get a new set of possible subkeys $\{2, 13\}$.

Looking at each of our sets of possible subkeys $\{12, 13, 14, 15\}$ and $\{2, 13\}$, we see that only 13 appears in both, so 13 has been correctly identified as the subkey being used.

2)
The key and the ciphertext do not determine the plaintext uniquely, so the formula $H(K|C) = H(K) + H(P) - H(C)$ cannot be used.
Thus, we compute $H(K|C)$ using the formula

$$H(X|Y) = -\sum_x \sum_y p(y) \cdot p(x|y) \log_2 p(x|y)$$

$p(c = 1) = \frac{1}{6} + \frac{1}{8} = \frac{7}{24}$

$p(c = 2) = \frac{1}{12} + \frac{1}{4} + \frac{1}{12} = \frac{5}{12}$

$p(c = 3) = \frac{1}{24} + \frac{1}{12} = \frac{1}{8}$

$p(c = 4) = \frac{1}{24} + \frac{1}{8} = \frac{1}{6}$

$p(k_1|c=1) = \frac{2}{3}$
$p(k_2|c=1) = \frac{1}{3}$
$p(k_3|c=1) = 0$
$p(k_1|c=2) = \frac{4}{5}$
$p(k_2|c=2) = \frac{1}{5}$
$p(k_3|c=2) = 0$
$p(k_1|c=3) = 0$
$p(k_2|c=3) = \frac{1}{3}$
$p(k_3|c=3) = \frac{2}{3}$
$p(k_1|c=4) = 0$
$p(k_2|c=4) = 0$
$p(k_3|c=4) = 1$
so, we can compute as:
$H(K|C) = -(\frac{7}{24}\left(\frac{2}{3}\log_2\left(\frac{2}{3}\right) + \frac{1}{3}\log_2\left(\frac{1}{3}\right)\right)$
$+ \frac{5}{12}\left(\frac{4}{5}\log_2\left(\frac{4}{5}\right) + \frac{1}{5}\log_2\left(\frac{1}{5}\right)\right)$
$+ \frac{1}{8}\left(\frac{1}{3}\log_2\left(\frac{1}{3}\right) + \frac{2}{3}\log_2\left(\frac{2}{3}\right)\right)$
$+ \frac{1}{6}\left(1\log_2\left(1\right)\right))$
$\approx 0.683426637059.$

$H(K|C) \approx 0.683426637059$