

1.

$$A \rightarrow 0 : 2, 4, 8, E$$

$$A \rightarrow 1 : 3, 9$$

$$A \rightarrow 2 : 1, B$$

$$A \rightarrow 3 : 0, A, 5, F, 6, C, 7, D$$

Now suppose two inputs of 5 and F which xor to A and output as 3

$$S0L = S0E \oplus S0K$$

$$S0k = S0E \oplus S0L$$

$$0 \oplus 5 = 5$$

$$A \oplus 5 = f$$

$$B \oplus 5 = 3$$

$$C \oplus 5 = 9$$

$$7 \oplus 5 = 2$$

$$D \oplus 5 = 8$$

$$F \oplus 5 = A$$

$$5 \oplus 5 = 0$$

$$0 \oplus F = f$$

$$A \oplus F = 5$$

$$B \oplus F = 9$$

$$C \oplus F = 3$$

$$7 \oplus F = 8$$

$$D \oplus F = 2$$

$$F \oplus F = 0$$

$$5 \oplus F = A$$

Thus the possible keys are $\{5, f, 3, a, 2, 8, a, 0\}$ which can be narrowed down further by repeating this process

2.

$$H(K|C) = H(K) + H(P) - H(C)$$

$$H(X) = - \sum_{i=1}^n p_i \log_2 p_i$$

$$H(K) = H(X)|X = \frac{1}{2}, \frac{1}{4}, \frac{1}{4} = 1.5$$

$$H(K) = H(X)|X = \frac{1}{3}, \frac{1}{6}, \frac{1}{2} = 1.459$$

$$P_C(C_i) = \sum_{\forall e_{k_i}(p_j)=C_i} P(k_i) * P(p_j)$$

$$H(C) = H(X)|X = \frac{7}{24}, \frac{5}{12}, \frac{1}{8}, \frac{1}{6} = 1.851$$

$$H(K) + H(P) - H(C) = 1.108$$