Ryan Berlin
Cryptography and Network Security
Homework 1 part 2

1.

A DiffCrypto attack would work by first constructing a Differential Distribution table for S_0. Then, assume we know two inputs S_E and S_K such that $S_E \oplus S_K = S_I$, and the output XOR is S_O. We can then look to the table for row S_I and column S_O, and this will give us a list of different input combinations. Finally, we XOR each of these values from the table with S_E and S_K to get a list of possible keys, removing duplicates from these lists. This process can be repeated with different values for S_E and S_K, and the true key will be in both of the resulting steps, so by repeating this process multiple times, we can narrow down the set of possible keys until there is only one true key remaining.

2.

$$H(P) = -\sum_{i=1}^{3} P(P = p_i) \log_2 P(P = P_i)$$
$$H(P) = -(\frac{1}{3}\log_2\frac{1}{3} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{2}\log_2\frac{1}{2})$$
$$H(P) = 1.459$$

$$H(K) = -\sum_{i=1}^{3} P(K = k_i) \log_2 P(K = k_i)$$
$$H(K) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4})$$
$$H(K) = 1.5$$

$$P_c(1) = \left(\frac{1}{2}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{2}\right) = \frac{7}{24}$$
$$P_c(2) = \left(\frac{1}{2}\right)\left(\frac{1}{6}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) = \frac{5}{12}$$
$$P_c(3) = \left(\frac{1}{4}\right)\left(\frac{1}{6}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) = \frac{1}{8}$$
$$P_c(4) = \left(\frac{1}{4}\right)\left(\frac{1}{6}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{2}\right) = \frac{1}{6}$$

$$H(C) = -\sum_{i=1}^{3} P(C = c_i) \log_2 P(C = c_i)$$
$$H(C) = -(\frac{7}{24}\log_2\frac{7}{24} + \frac{5}{12}\log_2\frac{5}{12} + \frac{1}{8}\log_2\frac{1}{8} + \frac{1}{8}\log_2\frac{1}{6})$$
$$H(C) = 1.851$$

$$H(K|C) = H(K) + H(P) - H(C)$$
$$H(K|C) = 1.5 + 1.459 - 1.851$$
$$\boldsymbol{H(K|C) = 1.108}$$