Liam Donohoe
Crypto HW1.2

1. Diff Crypto Attack: Using sBox0, we will look at the input string 7 to attempt to determine the key.

   When input into the sBox with all possible key values, the output is as follows:

   7 => 0: {3, 5}

   7 => 1: {0, 7, 11, 14}

   7 => 2: {1, 4, 8, 13}

   7 => 3: {2, 6, 9, A, C, F}

   Using this, we will take values 6 and A from the set that XORed to 3, and determine possible keys

   $S_0L = S_0K \oplus S_0E$

   $S_0K = S_0L \oplus S_0E$

$2 \oplus 6 = 4$	$2 \oplus A = 8$
$6 \oplus 6 = 0$	$6 \oplus A = C$
$9 \oplus 6 = F$	$9 \oplus A = 3$
$A \oplus 6 = B$	$A \oplus A = 0$
$C \oplus 6 = A$	$C \oplus A = 6$
$F \oplus 6 = 9$	$F \oplus A = 5$

   This gives us a possible key set of {0, 3, 4, 5, 6, 8, 9, A, B, C, F}. This set is still rather large, but is narrowed down from the original. If this same process were done on a value that had an even less uniformly distributed sBox output, then the key set would be even smaller. This process can be repeated further to decrease the possible keys even more as well.

2. $H(K \mid C) = H(K) + H(P) - H(C)$

$H(K) = -(\frac{1}{2} \log_2(\frac{1}{2}) + \frac{1}{4} \log_2(\frac{1}{4}) + \frac{1}{4} \log_2(\frac{1}{4}))$

$= -(-\frac{1}{2} + -\frac{1}{2} + -\frac{1}{2}) = 1.5$

$H(P) = \frac{1}{3} \log_2(\frac{1}{3}) + \frac{1}{6} \log_2(\frac{1}{6}) + \frac{1}{2} \log_2(\frac{1}{2})$

$= 1.46$

$H(C) = P(1) = \frac{1}{6} + \frac{1}{8} = 7/24$

$P(2) = 1/12 + 1/12 + \frac{1}{4} = 5/12$

$P(3) = 1/12 + 1/24 = 3/24 = \frac{1}{8}$

$P(4) = 1/24 + \frac{1}{8} = \frac{1}{6}$

$= 7/24\log_2(7/24) + 5/12\log_2(5/12) + ⅛ \log_2(⅛) + ⅙ \log_2(⅙)$
$= 1.85$

$H(K) + H(P) - H(C) = 1.5 + 1.46 - 1.85 = 1.11$