HW 1 pt2

Nolan Pofi

1. See DiffCrypto.py

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

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

$H(K) = -(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4}) = 1.5$
$H(P) = -(\frac{1}{3}\log_2\frac{1}{3} + \frac{1}{6}\log_2\frac{1}{6} + \frac{1}{2}\log_2\frac{1}{2}) = 1.46$
$H(K) = -(\frac{7}{24}\log_2\frac{7}{24} + \frac{5}{12}\log_2\frac{5}{12} + \frac{1}{8}\log_2\frac{1}{8} + \frac{1}{6}\log_2\frac{1}{6}) = 1.85$

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