Homework 1. Part 2.

Q1. [25pnts]For the simplified DES, consider Sbox S_0 and show how DiffCrypto attack would work. Show your work for partial credit.

Q2. [25pnts] Consider the crypto system below and compute H(K|C)

- P={a,b,c} with $P_P(a)=1/3$ $P_P(b)=1/6$ $P_P(c)=1/2$
- *K* = (k_1,k_2,k_3) with $P_K(k_1)=1/2$ $P_K(k_2)=1/4$ $P_K(k_3)=1/4$
- C = {1,2,3,4}

$$e_{k_1}(a)=1 \quad e_{k_1}(b)=2 \quad e_{k_1}(c)=2$$
$$e_{k_2}(a)=2 \quad e_{k_2}(b)=3 \quad e_{k_2}(c)=1$$
$$e_{k_3}(a)=3 \quad e_{k_3}(b)=4 \quad e_{k_3}(c)=4$$