Q1. [25pnts]For the simplified DES, consider Sbox S0 and show how DiffCrypto attack would work. Show your work for partial credit.

Table 1

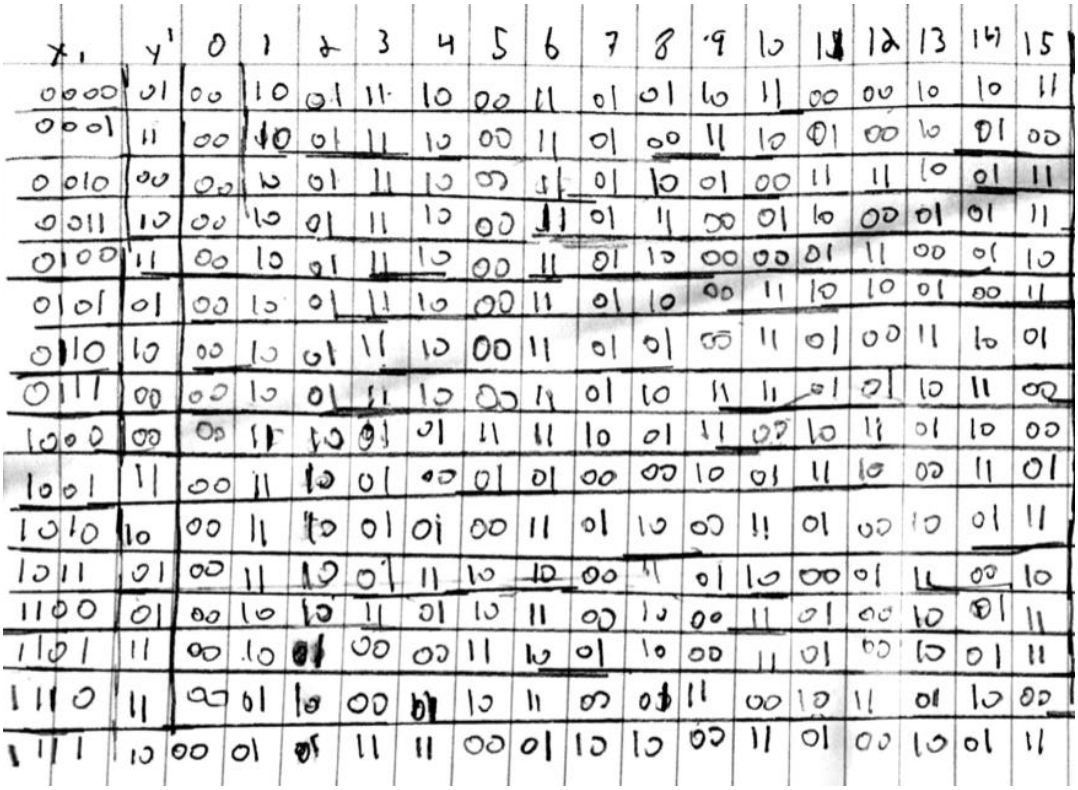
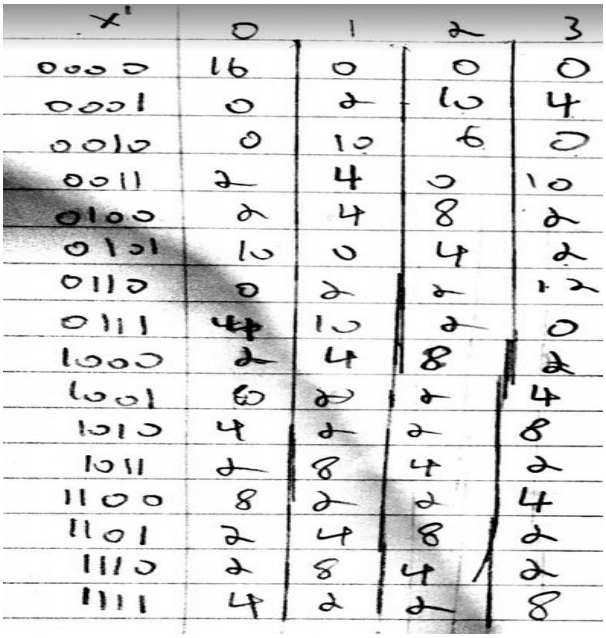


Table 2



For the differential crytoanalysis attack you first select a pair of inputs and you obtain the encrypted output of those inputs. The pair should (x, x*) such that X XOR X* = X' from table 1. Then create a list of inputs from Table 1 that can match the XOR of X and X*. This leave you with a list of possible keys.Repeat the above process with a different pair of inputs. Then you compare the set of possible keys between the 2 input pairs and remove any keys that overlap. Repeat until only one key remains, this is your key.

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