Linear Sbox will lead to relationship between ciphertext and plaintext.

<https://crypto.stackexchange.com/questions/53751/non-linearity-of-an-sbox>

we already know the first block plaintext is “HITCTF20”,and then we manually make a pair of c and m with any key,and do xor function between ciphertext,and we can recover the plaintext.

|  |
| --- |
| from baby\_des import decrypt,encrypt  import os  from Crypto.Util.strxor import strxor  key = os.urandom(16)  m='12345678'  m1='HITCTF20'  c1='e8e2d4985cbe2205'.decode('hex')  c2='5041bba9dab1b5bb'.decode('hex')  c3='4ce2d6de4e27bdec'.decode('hex')  c4='4e648ebd3b5112f4'.decode('hex')  #e8e2d4985cbe22055041bba9dab1b5bb4ce2d6de4e27bdec4e648ebd3b5112f4  y=encrypt(m,key)  m2=strxor(m1,strxor(m,decrypt(strxor(y,strxor(c1,c2)),key)))  m3=strxor(m1,strxor(m,decrypt(strxor(y,strxor(c1,c3)),key)))  m4=strxor(m1,strxor(m,decrypt(strxor(y,strxor(c1,c4)),key)))  m = m1+m2+m3+m4  print(m) |