Ex 1)

a. First and last bit decides row of S_1, while the rest decides column. The function is linear for input (x, y) if $S(x)+S(y)=S(x+y)$.

   $(x, y)=(000000, 000001)$: $row_x=00=0, col_x=0000=0$

   $row_y=01=1, col_y=0000=0$ $S(x)=14$ $S(y)=0$

   $S(x+y)=S(000001)=S(y)=0$ $\rightarrow Not\ linear$ $(x, y)=(111111, 100000)$

   $row_x=11=3, col_x=1111=15$ $row_y=10=2, col_y=0000=0$ $S(x)=13$

   $S(y)=4$ $S(x+y)=S(011111)=8$ $\rightarrow Not\ linear$

   $(x, y)=(101010, 010101)$ $row_x=10=2, col_x=0101=5$

   $row_y=01=1, col_y=1010=10$ $S(x)=6$ $S(y)=12$

   $S(x+y)=S(101010+010101)=S(111111)=13$ $\rightarrow Not\ linear$

b. See python code

c. See python code

Ex 2)

Verify $IP\left(IP^{-1}(x)\right)=x$ for $\left(x_1, x_2, x_3, x_4, x_5\right)$:

$IP(x_1) \to x_{58}$ $IP^{-1}(x_{58}) \to x_1$ $IP(x_2) \to x_{50}$ $IP^{-1}(x_{50}) \to x_2$ $IP(x_3) \to x_{42}$

$IP^{-1}(x_{42}) \to x_3$ $IP(x_4) \to x_{34}$ $IP^{-1}(x_{34}) \to x_4$ $IP(x_5) \to x_{26}$ $IP^{-1}(x_{26}) \to x_5$

Ex 3)

3.1)

$P=(0,0,0,0\ldots,0)-64\,zeros$ $\quad K=(0,0,0,0\ldots,0)-64\,zeros$ Initial permutation:

$IP(P)=P$ All zero input

First round:

$L_i=(0,0,0\ldots,0)-32\,zeros$ $\quad R_i=(0,0,0\ldots,0)-32\,zeros$ $\quad K_i=(0,0,0\ldots,0)-48\,zeros$

$L_{i+1}=R_i \quad R_{i+1}=F(R_i, K_i)\,XOR\,L_i$

Feistel:

- Expansion
  - $R_i=E(R_i)=(0,0,0\ldots,0)-48\,zeros$
- XOR with Ki:
  - $R_i=R_i\,XOR\,K_i=(0,0,0,\ldots,0)-48\,zeros$
- S_boxes:
  - Assuming every s_box = S_1 :
  - Every s_box outputs 14 = 1110
  - $R_i=(1,1,1,0,1,1,1,0\ldots)-1110\times 8$
- Permutation:
  - $P(R_i)=(0,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,0,0,1,0,1,1,1,1,1,1,1,1,1,0,1)$
- $R_i\,XOR\,L_i$:
  - $R_i\,XOR\,L_i=R_i(L_i\,is\,all\,zeros)$

$Output=(L_{i+1}, R_{i+1})$ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
0,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,0,0,1,0,1,1,1,1,1,1,1,1,1,0,1

3.2)

Since only one bit gets flipped, the first round is almost the same. Here I am just listing the differences.

$$P(x_{57})=1 \qquad \rightarrow IP(P) \rightarrow x_{63}=1$$

First round:

$$R_i \rightarrow x_{31}=1$$

Feistel:

$$Expansion\,E(R_i) \rightarrow x_{46}=1 \qquad XOR\,wit\,h\,K_i - No\,c\,h\,ange$$

$S\,boxes: Last\,six\,bits\,of\;R_i=(0,0,0,1,0,0) \rightarrow S(R_{last\,six\,bits})=13=1101$ $\quad R_i$ after the S boxes is the same as in the last, except the last four bits are 1101 instead of 1110.

$$Permutation: P(R_i)=(0,1,0,1,1,0,0,1,1,1,1,1,1,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,1)$$

$$R_i\,XOR\,L_i=R_i(L_i\,is\,still\,all\,zeros)$$

$Output=(L_{i+1},R_{i+1})$ $\quad$ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, ¿¿
0,1,0,1,1,0,0,1,1,1,1,1,1,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,1 ¿

As we can see, only a few bits flipped differently when we changed only one bit in the plaintext.

3.3)

Nothing will be different from 3.1 until we XOR with the key in the Feistel network.

Round 1 key generation:

$K=(1,0,0,0,\dots,0)-length\,64 \quad PC-1: K \rightarrow Remove\,8\,parity\,b\check{i}ts, all\,of\,them\,0, which\,gives$

$K=(1,0,0,0,\dots,0)-length\,56 \quad K=(C_i, D_i) \quad C_i=(1,0,0,0,\dots,0)-length\,28$

$D_i=all\,zeros-length\,28 \quad Since\,i\,t's\,round\,1, C_i \wedge D_i\,are\,¿\,by\,1, which\,gives:$

$C_i=(0,0,0\dots,0,1), C(x_{28})=1\,(same\,length) \quad D_i-same\,as\,before$

$Permuting\,K_i\,followin\,PC-2, we\,get: \quad PC-2(K_i) \rightarrow K(x_{37})=1$

The position of the 1 gets permuted from x_{28} to x_{37} of the key.

Feistel:

$R_i\,XOR\,K_i=K_i, since\,R_i\,is\,only\,zeros$

$S\,box: since\,R_i(x_{37}, x_{38}, x_{39}, x_{40}, x_{41}, x_{42})=(1,0,0,0,0,0)$ the 7th S_box will be different from 3.1.

The seventh S_box outputs 4 = 0100, which slightly affects the permutation.

$R_i=S(R_i)=(11101110111011101110111001001110)$

$R_i=P(R_i)=(0,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,0,1,0,1,1,1,1,1,1,1,1,0,0)$

$Output=(L_{i+1}, R_{i+1})$ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, ¿¿
0,1,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,0,1,0,1,1,1,1,1,1,1,1,0,0 ¿

As we can see again, only one bit difference in the key does not change much from 3.1 after only one round.

Ex 4)

See python file