CSCI971 Advance Computer Security: Homework #4

Mei Wangzhihui
2019124044

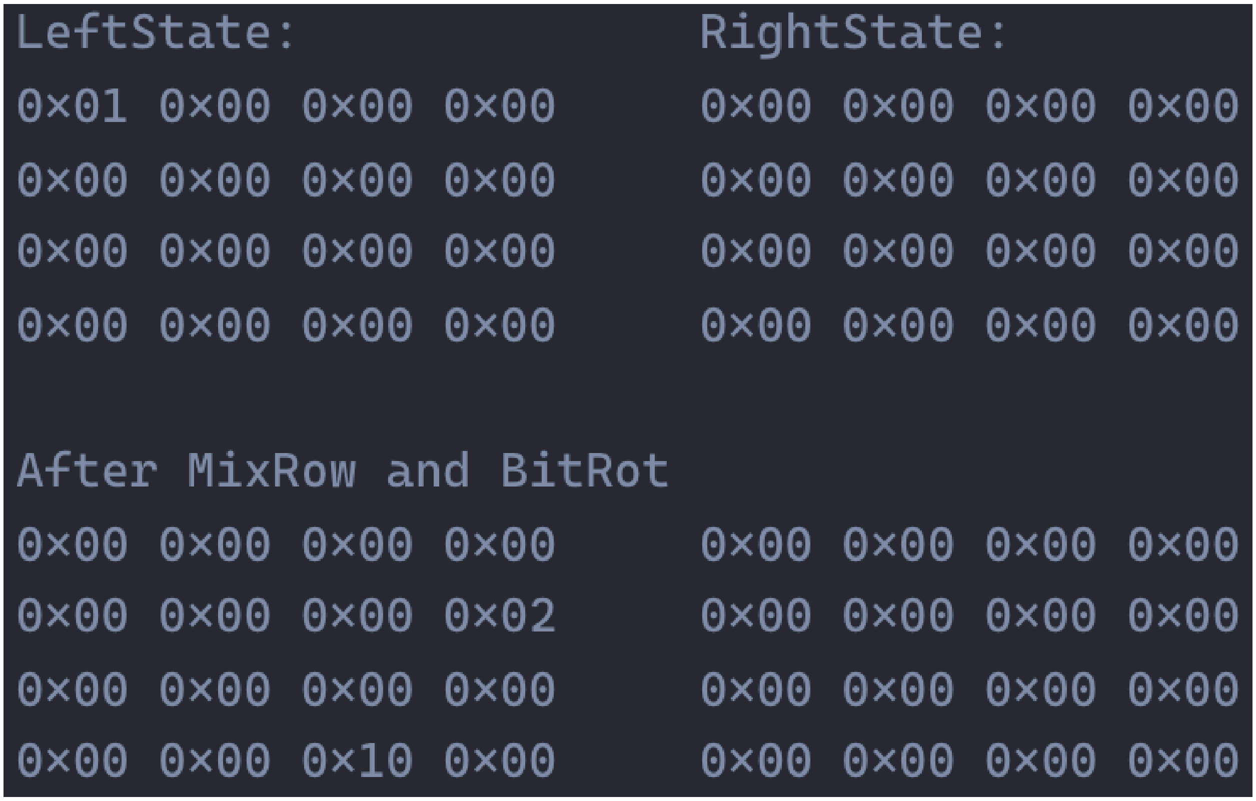
Problem 1

First, generate differential table for 3-bit Sbox Table **??** and 5-bit Sbox Table **??**;

	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0
4	0	0	0	0	2	2	2	2
5	0	2	0	2	2	0	2	0
6	0	0	2	2	2	2	0	0
7	0	2	2	0	2	0	0	2

Table 1: Differential distribution table for 3-bit Sbox

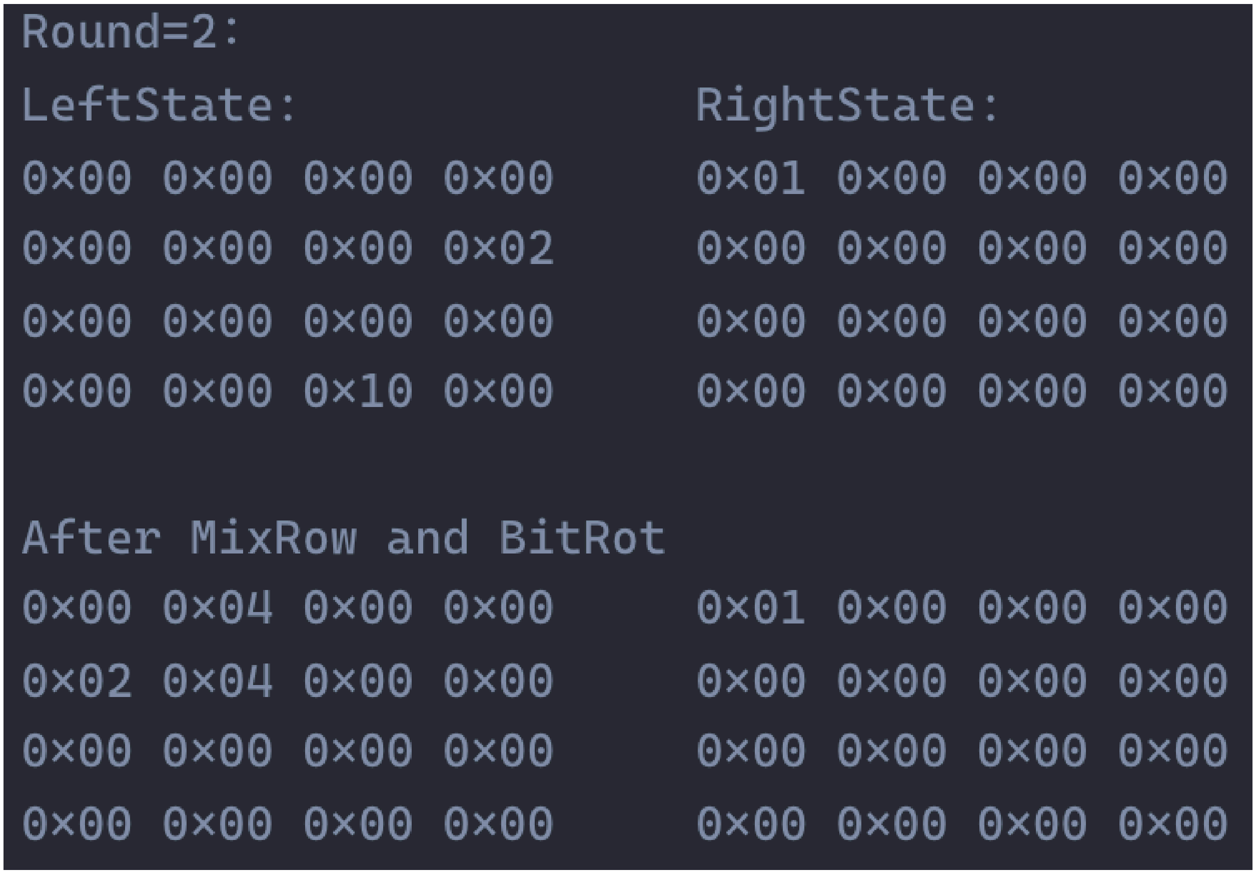
We set Table 1 as T1, Table 2 as T2:
We can find some extremum value point. T1(1,1), T1(2,2), T1(4,4), T2(1,1), T2(2,2), T2(4,4), T2(8,8), T2(16,16) with the Probability 1/4 to maintain its input differential value.
Because only Sbox can contribute to changes to differential value based on probability, the MixRow and BitRot change the differential value in a fixed mode (with the probibility of 1). We can just take Sbox into concern.
We can enumerate the input differential value 0x01, 0x02, 0x04, 0x08, 0x10 to the Sbox to get the best probibility path.
Then we can find when the p_0 of plaintext is $0x20$, we can attack as much as round. The plaintext = 0x20 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 .
In the First Round:
See figure **??**.
Round1
After entering the Sbox, the p_0 state has the probibility of $2/8 = 2^{-2}$ to maintain 0x01.
Maintain value probability $P_2 = 1/4 = 2^{-2}$
Round2
We have 0x02 0x10 and 0x01.
Maintain value probability $P_2 = 1/4 * 1/4 * 1/4 = 2^{-6}$



```
LeftState:                   RightState:
0x01 0x00 0x00 0x00          0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00          0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00          0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00          0x00 0x00 0x00 0x00

After MixRow and BitRot
0x00 0x00 0x00 0x00          0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x02          0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00          0x00 0x00 0x00 0x00
0x00 0x00 0x10 0x00          0x00 0x00 0x00 0x00
```

Figure 1: Round 1



```
Round=2:
LeftState:                  RightState:
0×00 0×00 0×00 0×00         0×01 0×00 0×00 0×00
0×00 0×00 0×00 0×02         0×00 0×00 0×00 0×00
0×00 0×00 0×00 0×00         0×00 0×00 0×00 0×00
0×00 0×00 0×10 0×00         0×00 0×00 0×00 0×00

After MixRow and BitRot
0×00 0×04 0×00 0×00         0×01 0×00 0×00 0×00
0×02 0×04 0×00 0×00         0×00 0×00 0×00 0×00
0×00 0×00 0×00 0×00         0×00 0×00 0×00 0×00
0×00 0×00 0×00 0×00         0×00 0×00 0×00 0×00
```

Figure 2: Round 2

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	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	8	0	8	0	8	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	8	0	0	0	8	0	0	0	8	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	8	0	0	0
5	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4
6	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	0
7	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
8	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4
10	0	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4
11	0	4	4	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	4	4	0
12	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0
13	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0	0	0	0	0	4	0	0	4	4	0	0	4	0	0	0	0
14	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
15	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	8	8	8	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4	4	4	4	4	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0	0	0	4	4
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
20	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4
21	0	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	4	0	4	0	0	0	0	0	0	0	0	0	4	0	4	0
22	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0	0	0	0	0	4	0	4	0	0	0	0	0	4	0	4	0	0
23	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0
24	0	0	0	0	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4	0	0	0	0
25	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
26	0	0	0	0	0	0	0	0	4	4	0	0	0	0	4	4	4	4	0	0	0	0	4	4	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0
28	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
29	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	0	0	0	0
30	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2	0	0
31	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2

Table 2: Differential distribution table for 5-bit Sbox