CSCI971 Advance Computer Security: Homework #4

Mei Wangzhihui
2019124044

Problem 1

First, generate differential table for 3-bit Sbox Table 1 and 5-bit Sbox Table 2;

	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

Then, set plaintext pair as:

	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