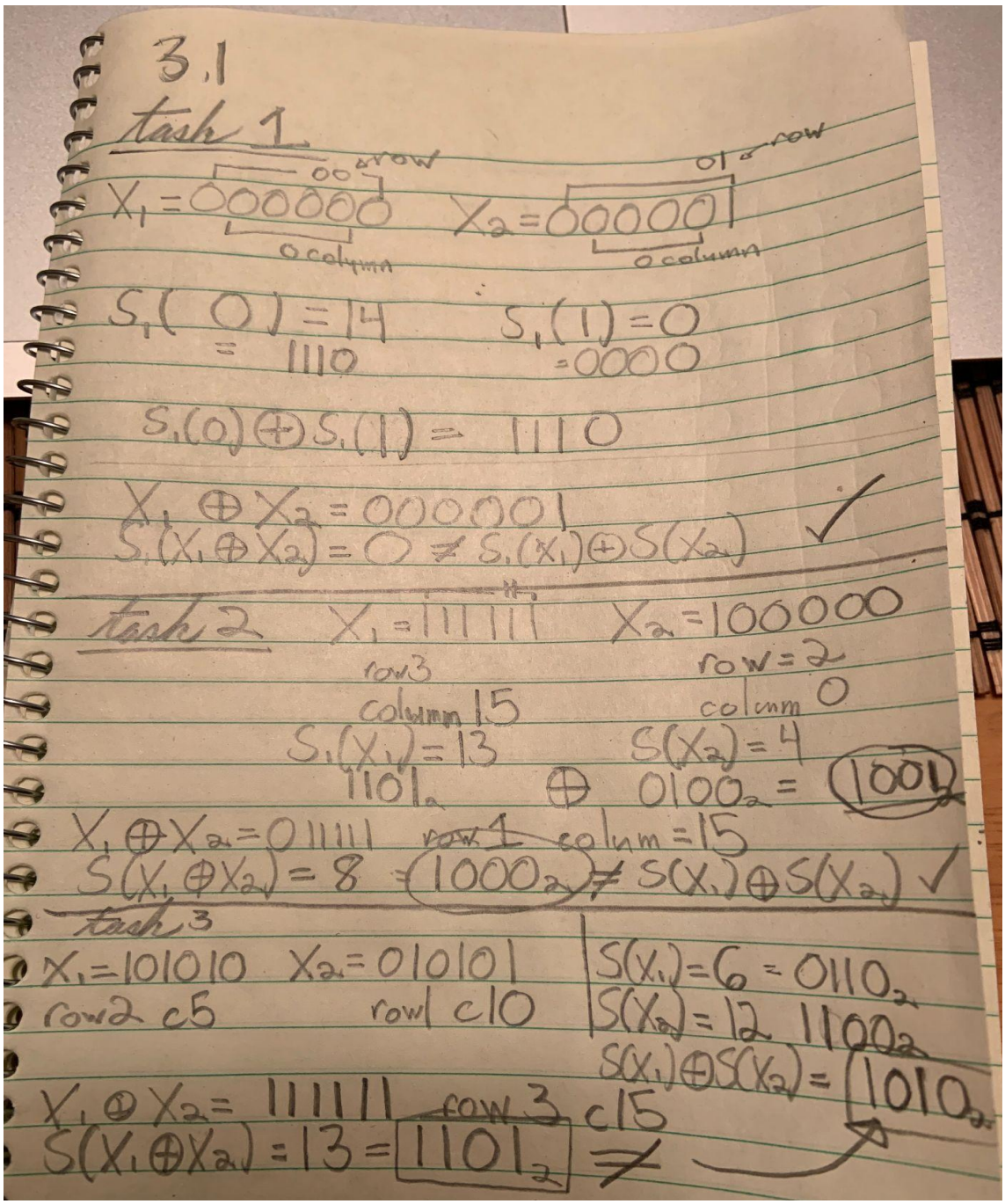
Carl Cortez
CIS 628
Chapter 3
Lab 5

3.1



3.2

Showing that $IP^{-1}(IP(x)) = x$ for the first five bits of x.

IP							
58	50	42	34	26	18	10	2

IP(1)=58 and IP^{-1}(58)=1

IP(2)=50 and IP^{-1}(50)=2

IP(3)=42 and IP^{-1}(42)=3

IP(4)=34 and IP^{-1}(34)=4

IP(5)=26 and IP^{-1}(26)=1

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

3.3

We know that the plaintext and key are filled with zeros. This will make the left side work be 0000 0000.

From the tables in the textbook, below are the outcomes when assessing inputs of 0:

S_1	0
0	14

S_2	0
0	15

S_3	0
0	10

S_4	0
0	07

S_5	0
0	02

S_6	0
0	12

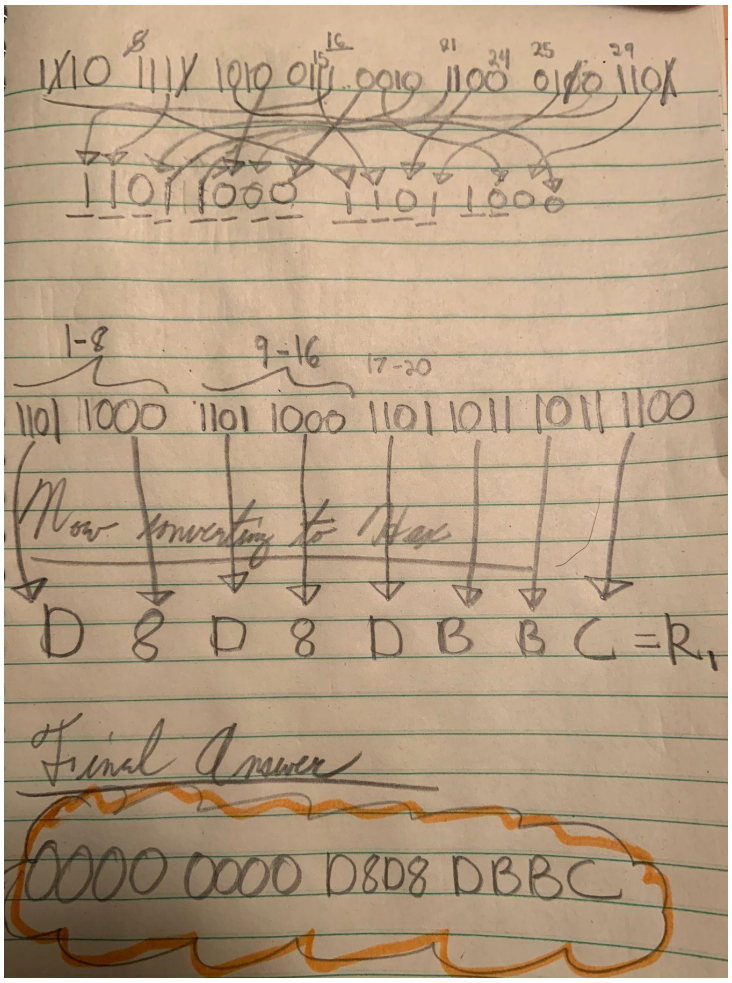
S_7	0
0	04

S_8	0
0	13

In binary:

1110 1111 1010 0111 0010 1100 0100 1101

Now using the P table:



3.5

We have an input work of 1 at position 57. The other bits and the key are 0. From the IP table, bit 57 maps to position 33; the first position in R_0.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1

From the E table, we see that 1 is in position 2 and the final 48th position.

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

S_1= 0 1 0 0 0 0 and S_8= 0 0 0 0 0 1; these are the only unique inputs for this round.

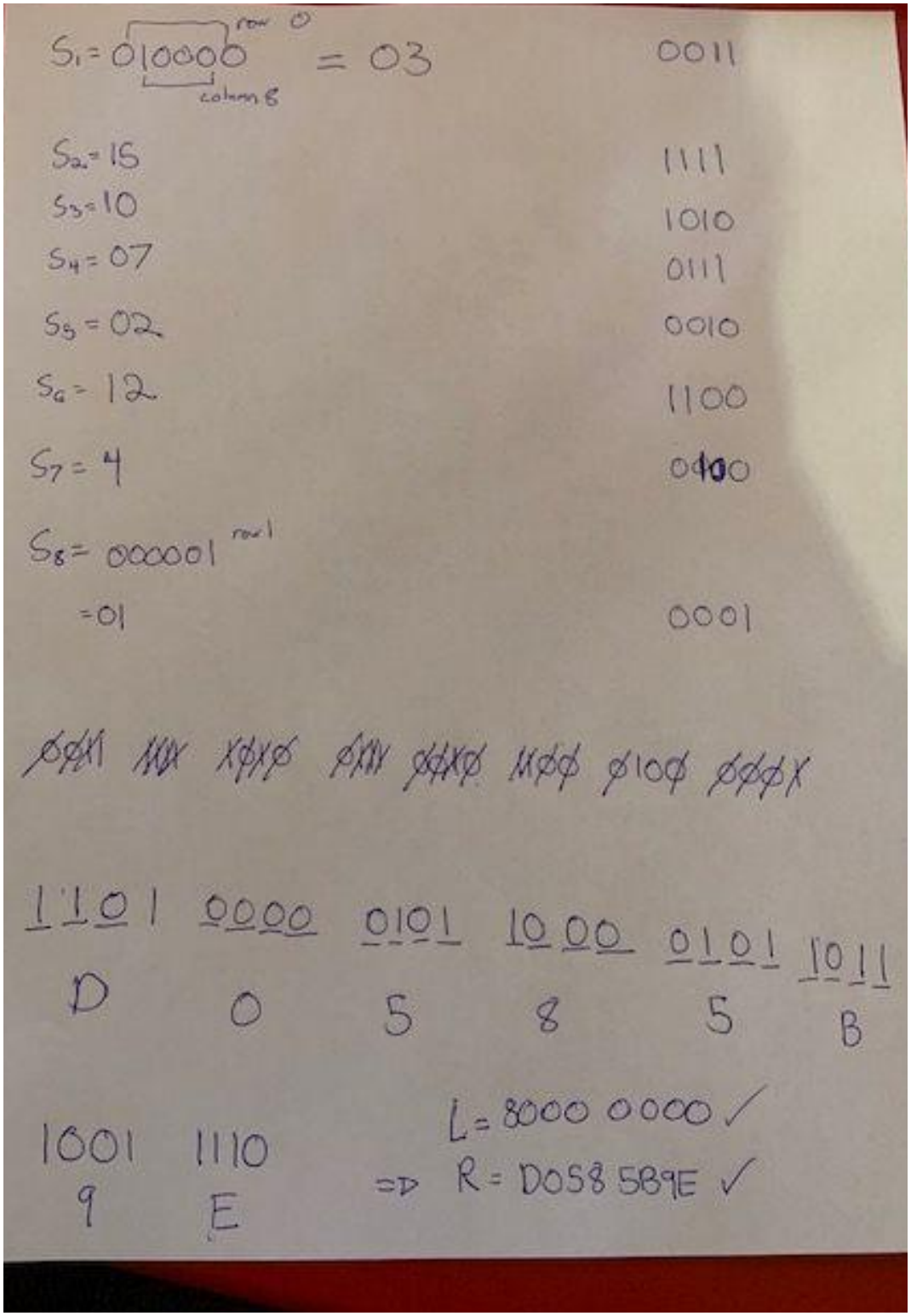
Task A

Two S-boxes get different inputs. s1=010000 and s2=000001. The inputs are 0's.

Task B

The minimum number of output bits that change according to S-box design criteria would be 4 bits.

Task C



Task D

Comparing to the previous task with all 0's:

- Our S_1 output differs; 1110 vs. 0011.

- Our S_8 output differs; 1101 vs. 0001.
- Our left half changes from 0000 to 8000

This totals to 3+2+1=6 changes for the output bits after the first round.

3.6

$PC-1$							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

From PC-1, position 1 is moved to 8.
A half of the key is all 0's.
The other half uses the fact that position 1 moved to 8. This produces 01000000_{16}
To Be Continued.

3.9

We have plaintext and ciphertext as we plan a known-plaintext attack against DES. Our worst case scenario would occur if we've scanned through all potential combos and the final key happens to match. With 56 spots and two options in each spot, we would have to check 2^{56} keys.

On average, we assume that our key search success happens around the halfway mark of our search. Splitting these opportunities in 2: $\frac{2^{56}}{2} = 2^{56-1} = 2^{55}$.

2^{55} key checks on average.