Contributors: Hanliang Jiang hjiang38@binghamton.edu B00714328
SiYu Liu sliu121@binghamton.edu B00704610

1. The message “dfsfhoisgosidh” using rail fence cipher with depth 4.

There are 14 characters.14 / 4 = 3 …2 so the first and the second row have 4 characters, the third and the forth has 3 characters.

d f s f
h o i s
g o s
i d h

The answer is dhgifoodsishfs

2.The message is “dhdplakshgiskfnhgd” using row transposition cipher and key: 351462.

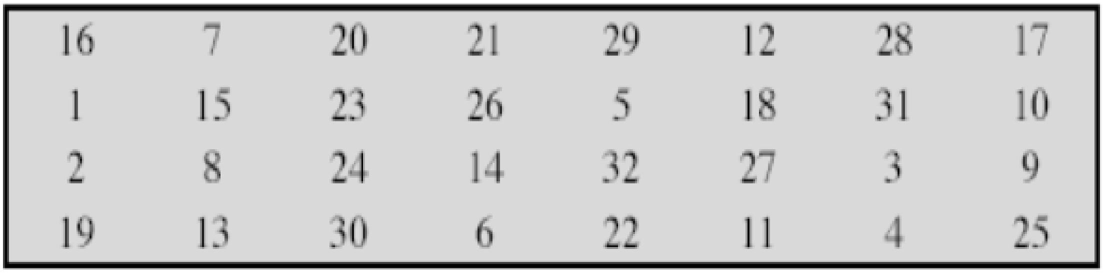
There are 18 characters.18 / 6 = 3.I put 3 characters in each column.The first key is 3, I put the first three characters in the third column so the third column is “dhd” then the fifth column, the first column ,the forth column, the sixth column and the second column.

1 2 3 4 5 6
k h d g p k
s g h i l   f
h d d s a n

The answer is khdgpksghilfhddsan

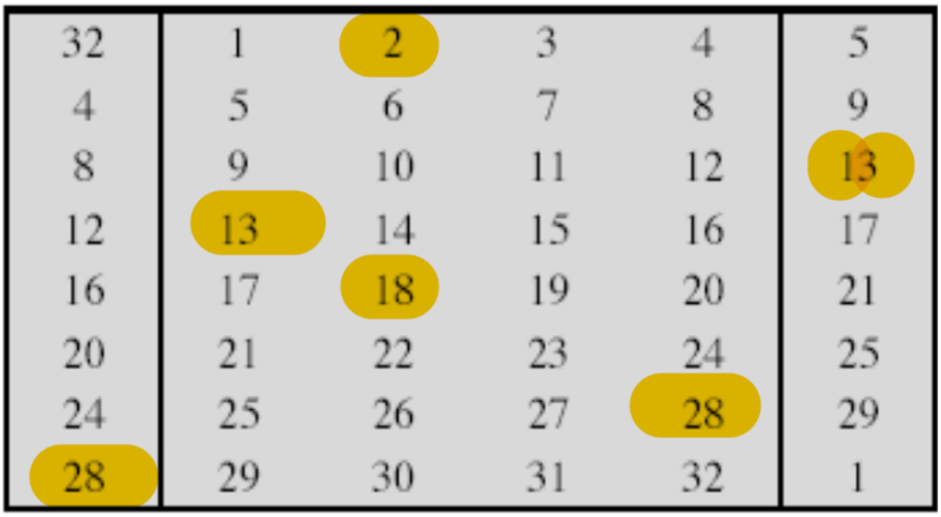
3.The s-box S2 outputs 4 bits which are 5th ,6th ,7th ,8th bit.

According to permutation function table,



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

It puts the 7th value (0 or 1) into the 2nd bit. It puts the 5th value into the 13th bit. It puts the 8th value into the 18th bit. It puts the 6th value into the 28th bit. Then L_{i-1} XOR the value and the R_i. In next round, R_i is R_{i-1}.Then R_{i-1} uses E table to change from 32 bits to 48 bits. According to E table, it shows there are 6 rows changing.



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

Each row means a s-box,there are 6 rows changing. It shows the four output bits from each S-box affect six different S-boxes on the next round.

4.According to the first plaintext-ciphertext pair,

L_{i-1} = 0000 0000 0000 0000 0000 0000 0000 0000

R_{i-1} = 0010 0000 0000 0000 0000 0000 0000 0000

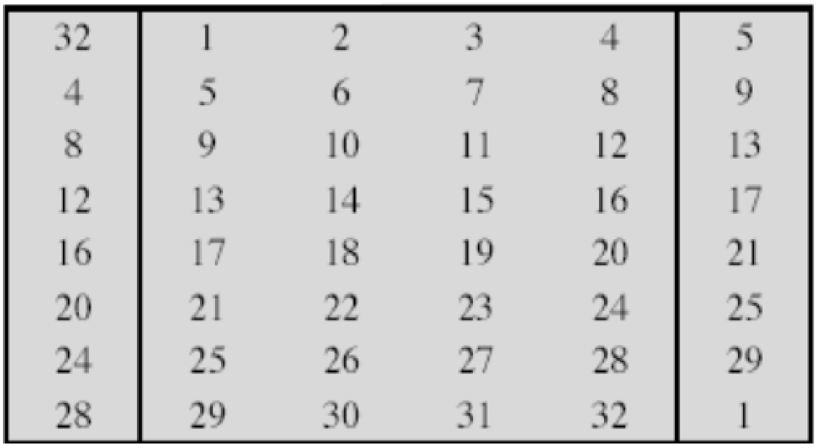
L_i = 0010 0000 0000 0000 0000 0000 0000 0000

R_i = 0011 0000 0000 0000 0000 0000 0000 0000

R_{i-1} is 32 bits now,after using expanded permutation it changes to 48 bits

0 0010 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0

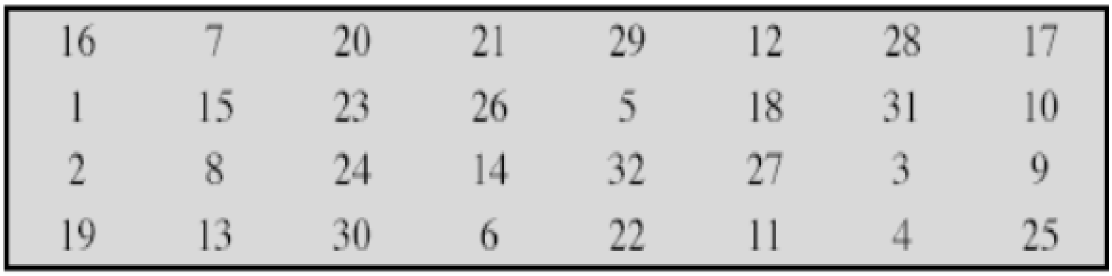
Expanded Permutation (E)



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

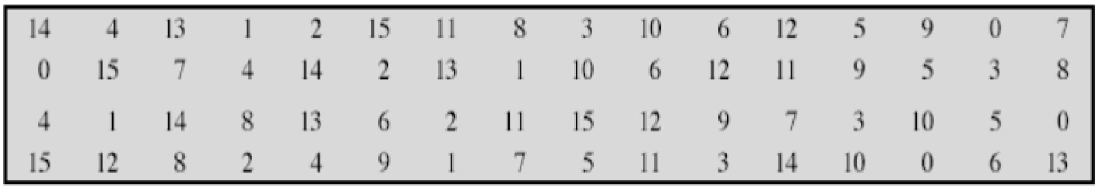
According to L_{i-1} XOR (the output of P) = R_i, the output of P table is:
0011 0000 0000 0000 0000 0000 0000 0000.

According to the S-box table,the output of S-box is:
0000 0000 0000 0000 0001 1000 0000 0000



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

The first four bits are 0000 so there are 4 possible inputs of S-box.They are 011100 or 000001 or 111110 or 111011.



14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

According to the second plaintext-ciphertext pair,

L_{i-1} = 0110 0000 1000 0000 1000 0000 0000 0000

R_{i-1} = 0100 0000 0000 0000 0000 0000 0000 0000

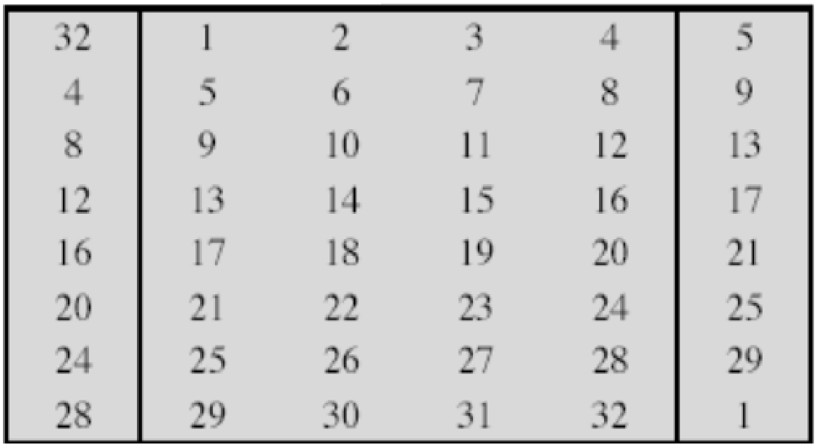
L_i = 0100 0000 0000 0000 0000 0000 0000 0000

R_i = 0110 0000 0000 0000 0000 0000 0000 0000

R_{i-1} is 32 bits now,after using expanded permutation it changes to 48 bits

0 0100 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0
0 0000 0

Expanded Permutation (E)



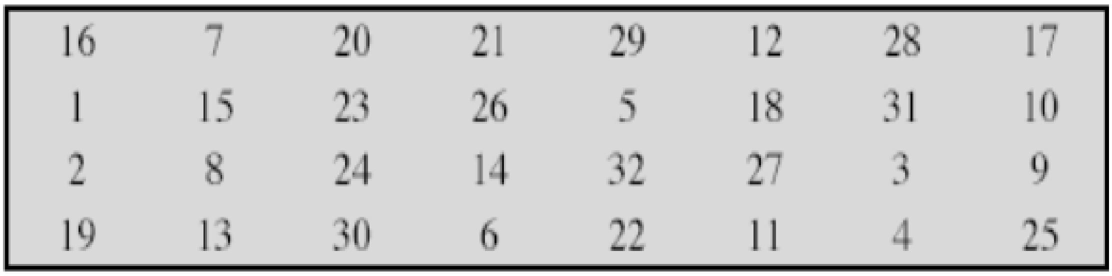
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

According to L_{i-1} XOR (the output of P) = R_i,the output of P table is:

0000 0000 1000 0000 1000 0000 0000 0000.

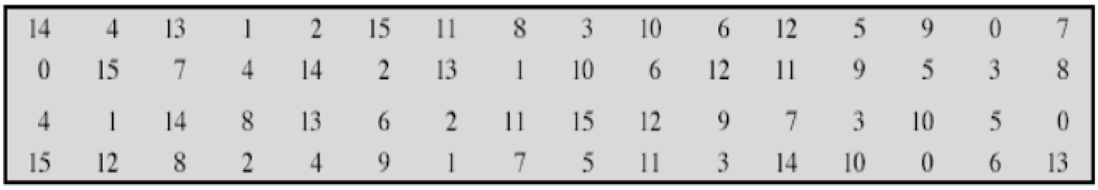
According to the S-box table,the output of S-box is:

1100 0000 0000 0000 0000 0000 0000 0000



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

The first four bits are 0000 so there are 4 possible inputs of S-box.They are 010110 or 010101 or 110010 or 100011.



14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

In the first plaintext-ciphertext pair,000100 XOR K_i = 011100 or 000001 or 111110 or 111011,so K_i = 011000 or 000101 or 111010 or 111111
In the second plaintext-ciphtext pair,001000 XOR K_i = 010110 or 010101 or 110010 or 100011,so K_i = 011110 or 011101 or 111010 or 101011.
So **K_i = 111010.**
5.According to Fermat's theorem,3 and 11 are relatively prime,so a = 3 p = 11,3^{10} %11 = 1.3^{300} % 11 = 3^{10} * 3^{10} * 3^{10} * …3^{10} % 11= 1(there are thirty 3^{10} multiplying together).As a result, the question 3^{302} % 11 = 3^{300} * 3^2 %11 = 9.